DeviceLock®

Manuale utente

Versione software 7.1

© 1996-2012 DeviceLock, Inc. Tutti i diritti riservati.

Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso. Nessuna porzione di questo documento può essere riprodotta né trasferita in qualsiasi forma e con qualsiasi mezzo a fini diversi dall'uso personale da parte dell'acquirente, senza la previa autorizzazione scritta da parte di DeviceLock, Inc.

Marchio di fabbrica

DeviceLock e il logo di DeviceLock sono marchi di fabbrica registrati di DeviceLock, Inc. Tutti gli altri nomi di prodotto, marchi di servizio e marchi di fabbrica citati in questo documento sono marchi di fabbrica dei rispettivi proprietari.

DeviceLock - Manuale utente
Versione software: 7.1
Aggiornamento: marzo 7, 2012

Sommario

INFORMAZIONI SU QUESTO MANUALE 6
CONVENZIONI TIPOGRAFICHE 6
INTRODUZIONE 7
INFORMAZIONI GENERALI 7
CONTROLLO GESTITO DELL'ACCESSO PER PERIFERICHE E PROTOCOLLI 11
INFORMAZIONI SU DEVICELOCK CONTENT SECURITY SERVER 16
FUNZIONAMENTO DI SEARCH SERVER 16
ESTENSIONE DELLE FUNZIONALITÀ DI DEVICELOCK CON CONTENTLOCK E NETWORKLOCK 18
LICENZE 22
MISURE DI PROTEZIONE DI BASE CONSIGLIATE 23
INSTALLAZIONE 25
RICHIESTE DI SISTEMA 25
DISTRIBUZIONE DI DEVICELOCK SERVICE 25
INSTALLAZIONE INTERATTIVA 25
INSTALLAZIONE AUTOMATICA 32
INSTALLAZIONE TRAMITE MICROSOFT SYSTEMS MANAGEMENT SERVER 34
INSTALLAZIONE REMOTA TRAMITE DEVICELOCK MANAGEMENT CONSOLE 34
INSTALLAZIONE REMOTA TRAMITE DEVICELOCK ENTERPRISE MANAGER 35
INSTALLAZIONE TRAMITE CRITERI DI GRUPPO 37
INSTALLAZIONE DELLE CONSOLE DI GESTIONE 46
INSTALLAZIONE DI DEVICELOCK ENTERPRISE SERVER 53
PROGETTAZIONE DELL'INFRASTRUTTURA 54
INSTALLAZIONE INTERATTIVA 54
INSTALLAZIONE DI DEVICELOCK CONTENT SECURITY SERVER 72
CERTIFICATI DI DEVICELOCK 82
INFORMAZIONI GENERALI 82
CREAZIONE DEI CERTIFICATI DI DEVICELOCK 82
INSTALLAZIONE/RIMOZIONE DEL CERTIFICATO DI DEVICELOCK 84
STRUMENTO DEVICELOCK SIGNING 89
INFORMAZIONI GENERALI 89
CODICE PERIFERICA (DEVICE CODE) 89
IMPOSTAZIONI DEL SERVIZIO 91
DEVICELOCK MANAGEMENT CONSOLE 95
INFORMAZIONI GENERALI 95
CENNI PRELIMINARI SULL'INTERFACCIA UTENTE 97
CONNESSIONE AI COMPUTER 98

POSSIBILI ERRORI DI CONNESSIONE 101

GESTIONE DI DEVICELOCK SERVICE 103
SEZIONE SERVICE OPTIONS 105
SEZIONE DEVICES 130
SEZIONE PERMISSIONS (REGULAR PROFILE) 131
SEZIONE AUDITING & SHADOWING (REGULAR PROFILE) 141
SEZIONE USB DEVICES WHITE LIST (REGULAR PROFILE) 151
SEZIONE MEDIA WHITE LIST (REGULAR PROFILE) 156
SEZIONE SECURITY SETTINGS (REGULAR PROFILE) 160
SEZIONE AUDIT LOG VIEWER (SERVIZIO) 164
SEZIONE SHADOW LOG VIEWER (SERVIZIO) 169

GESTIONE DI DEVICELOCK ENTERPRISE SERVER 176
SEZIONE SERVER OPTIONS (SERVER) 177
SEZIONE AUDIT LOG VIEWER (SERVER) 178
SEZIONE SHADOW LOG VIEWER (SERVER) 182
SEZIONE SERVER LOG VIEWER 187
MONITORAGGIO 190

GESTIONE E UTILIZZO DI DEVICELOCK CONTENT SECURITY SERVER 204
ESPLORAZIONE DI DEVICELOCK CONTENT SECURITY SERVER 204
CONFIGURAZIONE DELLE IMPOSTAZIONI GENERALI DI DEVICELOCK CONTENT SECURITY SERVER 207
CONFIGURAZIONE DELLA RICERCA FULL-TEXT PER SEARCH SERVER 213
UTILIZZO DI SEARCH SERVER 221

GESTIONE MEDIANTE I CRITERI DI GRUPPO 232

INFORMAZIONI GENERALI 232

APPLICARE I CRITERI DI GRUPPO 233

REGOLE DI EREDITARIETÀ STANDARD GPO 233

AVVIARE DEVICELOCK GROUP POLICY MANAGER 234

UTILIZZARE DEVICELOCK GROUP POLICY MANAGER 238

UTILIZZARE GRUPPO DI CRITERI RISULTANTE (RSOP) 241

DEVICELOCK SERVICE SETTINGS EDITOR 244

INFORMAZIONI GENERALI 244

DEVICELOCK ENTERPRISE MANAGER 246

INFORMAZIONI GENERALI 246

INTERFACCIA UTENTE 247

LA FINESTRA DI DIALOGO SCAN NETWORK 248
SELEZIONARE I COMPUTER 248
SELEZIONARE I PLUG-IN 255
AVVIARE UNA SCANSIONE 255

I PLUG-IN 256
PLUG-IN AUDIT LOG VIEWER 257
PLUG-IN INSTALL SERVICE 258
PLUG-IN REPORT PERMISSIONS/AUDITING 258
PLUG-IN REPORT PNP DEVICES 260

PLUG-IN SET SERVICE SETTINGS 261
PLUG-IN SHADOW LOG VIEWER 262
PLUG-IN UNINSTALL SERVICE 262

APRIRE, SALVARE, ESPORTARE I DATI RACCOLTI 263

CONFRONTARE I DATI 264

FILTRARE I DATI 268

REGOLE BASATE SUL CONTENUTO PER LE PERIFERICHE (REGULAR PROFILE) 271

REGOLE BASATE SUL CONTENUTO PER LE OPERAZIONI DI CONTROLLO DELL'ACCESSO 272

REGOLE BASATE SUL CONTENUTO PER LE OPERAZIONI DI COPIA SHADOW 276

CONFIGURAZIONE DELLE IMPOSTAZIONI DI RILEVAMENTO DEL CONTENUTO ... 277
GRUPPI DI CONTENUTO FILE TYPE DETECTION (RILEVAMENTO TIPO FILE) 278
GRUPPI DI CONTENUTO KEYWORDS (PAROLE CHIAVE) 282
GRUPPI DI CONTENUTO PATTERN (MOTIVI) 287
GRUPPI DI CONTENUTO DOCUMENT PROPERTIES (PROPRIETÀ DOCUMENTI) .. 291
GRUPPI DI CONTENUTO COMPLEX (COMPLESSI) 296
VISUALIZZAZIONE DEI GRUPPI DI CONTENUTO INCORPORATI 299
DUPLICAZIONE DEI GRUPPI DI CONTENUTO INCORPORATI 300
MODIFICA ED ELIMINAZIONE DEI GRUPPI DI CONTENUTO PERSONALIZZATI. 301
VERIFICA DEI GRUPPI DI CONTENUTO 302

GESTIONE DELLE REGOLE BASATE SUL CONTENUTO 303
DEFINIZIONE DELLE REGOLE BASATE SUL CONTENUTO 303
MODIFICA DELLE REGOLE BASATE SUL CONTENUTO 307
COPIA DELLE REGOLE BASATE SUL CONTENUTO 308
ESPORTAZIONE E IMPORTAZIONE DELLE REGOLE BASATE SUL CONTENUTO .. 309
RIMOZIONE DELLA DEFINIZIONE DELLE REGOLE BASATE SUL CONTENUTO ... 311
ELIMINAZIONE DELLE REGOLE BASATE SUL CONTENUTO 312

REGOLE BASATE SUL CONTENUTO PER I PROTOCOLLI (REGULAR PROFILE) 313

REGOLE BASATE SUL CONTENUTO PER LE OPERAZIONI DI CONTROLLO DELL'ACCESSO 313

REGOLE BASATE SUL CONTENUTO PER LE OPERAZIONI DI COPIA SHADOW 315

CONFIGURAZIONE DELLE IMPOSTAZIONI DI RILEVAMENTO DEL CONTENUTO ... 317
GRUPPI DI CONTENUTO FILE TYPE DETECTION (RILEVAMENTO TIPO FILE) 318
GRUPPI DI CONTENUTO KEYWORDS (PAROLE CHIAVE) 321
GRUPPI DI CONTENUTO PATTERN (MOTIVI) 326
GRUPPI DI CONTENUTO DOCUMENT PROPERTIES (PROPRIETÀ DOCUMENTI) .. 330
GRUPPI DI CONTENUTO COMPLEX (COMPLESSI) 334
VISUALIZZAZIONE DEI GRUPPI DI CONTENUTO INCORPORATI 338
DUPLICAZIONE DEI GRUPPI DI CONTENUTO INCORPORATI 338
MODIFICA ED ELIMINAZIONE DEI GRUPPI DI CONTENUTO PERSONALIZZATI . 339
VERIFICA DEI GRUPPI DI CONTENUTO 340

GESTIONE DELLE REGOLE BASATE SUL CONTENUTO 341
DEFINIZIONE DELLE REGOLE BASATE SUL CONTENUTO 341
MODIFICA DELLE REGOLE BASATE SUL CONTENUTO 345

COPIA DELLE REGOLE BASATE SUL CONTENUTO 346
ESPORTAZIONE E IMPORTAZIONE DELLE REGOLE BASATE SUL CONTENUTO .. 347
RIMOZIONE DELLA DEFINIZIONE DELLE REGOLE BASATE SUL CONTENUTO ... 349
ELIMINAZIONE DELLE REGOLE BASATE SUL CONTENUTO 350

PROTOCOLLI (REGULAR PROFILE) 352

GESTIONE DELLE AUTORIZZAZIONI PER I PROTOCOLLI 353
IMPOSTAZIONE E MODIFICA DELLE AUTORIZZAZIONI 357
RIMOZIONE DELLA DEFINIZIONE DELLE AUTORIZZAZIONI 359

GESTIONE DELLE REGOLE DI CONTROLLO E SHADOWING PER I PROTOCOLLI .. 360
DEFINIZIONE E MODIFICA DELLE REGOLE DI CONTROLLO E SHADOWING 369
RIMOZIONE DELLA DEFINIZIONE DELLE REGOLE DI CONTROLLO E SHADOWING 372

GESTIONE DELLA LISTA BIANCA DEI PROTOCOLLI 373
DEFINIZIONE DELLA LISTA BIANCA DEI PROTOCOLLI 377
MODIFICA DELLA LISTA BIANCA DEI PROTOCOLLI 380
COPIA DELLE REGOLE DELLA LISTA BIANCA DEI PROTOCOLLI 381
ESPORTAZIONE E IMPORTAZIONE DELLA LISTA BIANCA DEI PROTOCOLLI 382
RIMOZIONE DELLA DEFINIZIONE DELLA LISTA BIANCA DEI PROTOCOLLI 385
ELIMINAZIONE DELLE REGOLE DELLA LISTA BIANCA DEI PROTOCOLLI 385

GESTIONE DELLE IMPOSTAZIONI DI PROTEZIONE PER I PROTOCOLLI 386
DEFINIZIONE E MODIFICA DELLE IMPOSTAZIONI DI PROTEZIONE 387
RIMOZIONE DELLA DEFINIZIONE DELLE IMPOSTAZIONI DI PROTEZIONE 388

RAPPORTI DI DEVICELOCK 389

CATEGORIE E TIPI DI RAPPORTI 389
RAPPORTI AUDIT LOG 390
RAPPORTI SHADOW LOG 394

CONFIGURAZIONE DELL'INVIO DEI RAPPORTI TRAMITE E-MAIL 397

IMPOSTAZIONE DEL FORMATO PREDEFINITO PER I RAPPORTI 398

DEFINIZIONE DEI PARAMETRI DEL RAPPORTO 399
FINESTRA DI DIALOGO REPORT OPTIONS 399

GESTIONE DEI RAPPORTI 404
ESECUZIONE DEI RAPPORTI 405
AGGIORNAMENTO DEI RAPPORTI 406
VISUALIZZAZIONE DEI RAPPORTI 407
VISUALIZZAZIONE DEI PARAMETRI DEI RAPPORTI 407
ESPORTAZIONE E SALVATAGGIO DEI RAPPORTI 408
INVIO DEI RAPPORTI TRAMITE E-MAIL 409
ELIMINAZIONE DEI RAPPORTI 409

CRITERI DI PROTEZIONE DI DEVICELOCK (OFFLINE PROFILE) 411

CONFIGURAZIONE DELLE IMPOSTAZIONI DI RILEVAMENTO IN MODALITÀ OFFLINE 412

PASSAGGIO DALLA MODALITÀ ONLINE A QUELLA OFFLINE E VICEVERSA 414

GESTIONE DEI CRITERI DI PROTEZIONE OFFLINE PER LE PERIFERICHE 415
GESTIONE DELLE AUTORIZZAZIONI OFFLINE 415
GESTIONE DELLE REGOLE DI CONTROLLO E SHADOWING OFFLINE 420

GESTIONE DELLA LISTA BIANCA DELLE PERIFERICHE USB OFFLINE 425
GESTIONE DELLA LISTA BIANCA DELLE UNITÀ OFFLINE 432
GESTIONE DELLE REGOLE BASATE SUL CONTENUTO OFFLINE PER LE PERIFERICHE 439
GESTIONE DELLE IMPOSTAZIONI DI PROTEZIONE OFFLINE 450
GESTIONE DEI CRITERI DI PROTEZIONE OFFLINE PER I PROTOCOLLI 455
GESTIONE DELLE AUTORIZZAZIONI OFFLINE PER I PROTOCOLLI 456
GESTIONE DELLE REGOLE DI CONTROLLO E SHADOWING OFFLINE PER I PROTOCOLLI 460
GESTIONE DELLA LISTA BIANCA DEI PROTOCOLLI OFFLINE 465
GESTIONE DELLE REGOLE BASATE SUL CONTENUTO OFFLINE PER I PROTOCOLLI 476
GESTIONE DELLE IMPOSTAZIONI DI PROTEZIONE OFFLINE PER I PROTOCOLLI 487
TEMPORARY WHITE LIST 491
INTRODUZIONE 491
STRUMENTO TEMPORARY WHITE LIST AUTHORIZATION 492
APPENDICE 495
ESEMPI DI AUTORIZZAZIONI E CONTROLLO PER LE PERIFERICHE 495
ESEMPI DI AUTORIZZAZIONI 495
ESEMPI DI REGOLE DI CONTROLLO E DI SHADOWING 506
ESEMPI DI AUTORIZZAZIONI PER I PROTOCOLLI 509
ESEMPI DI REGOLE BASATE SUL CONTENUTO (CONTENT-AWARE RULES) 512

Informazioni su questo manuale

Questo manuale fornisce informazioni dettagliate sull'installazione e l'utilizzo di DeviceLock. Si rivolge principalmente ad amministratori, specialisti della protezione e altri professionisti del settore IT che si occupano della protezione dei dati all'interno di un'organizzazione.

Questo manuale presume una conoscenza di base del sistema operativo e dell'ambiente di rete Microsoft Windows e il fatto di saper creare una rete locale (LAN).

Convenzioni tipografiche

La seguente tabella illustra le convenzioni tipografiche utilizzate in questo manuale.

CONVENZIONE	DESCRIZIONE
Testo in grassetto	Indica gli elementi dell'interfaccia utente come menu, comandi, titoli delle finestre di dialogo e opzioni.
Testo in corsivo	Indica i commenti.
Testo in blu	Indica i collegamenti ipertestuali.
Nota	Indica informazioni aggiuntive.
Avviso	Indica la presenza di potenziali problemi.
Procedura consigliata	Indica le procedure consigliate.
Segno più (+)	Indica una combinazione di tasti da premere simultaneamente.

Introduzione

Informazioni generali

Quando si tratta di amministrare e garantire la protezione dei computer connessi ad una rete aziendale, è importante impedire il trasferimento e il download di software non autorizzato. Grazie a DeviceLock, non sarà più necessario proteggere fisicamente le unità floppy. Inoltre, DeviceLock introduce innumerevoli vantaggi.

DeviceLock è uno strumento facile da installare che consente agli amministratori di sistema di accedere rapidamente in modo remoto alle periferiche. L'amministratore della macchina o del dominio può concedere o negare l'accesso a unità floppy, CD-ROM e altri tipi di supporti rimovibili, unità a nastro, adattatori WiFi e Bluetooth, porte USB, FireWire, a infrarossi, seriali e parallele. DeviceLock supporta tutti i tipi di file system.

NetworkLock, un'estensione di DeviceLock, fornisce un controllo sulle comunicazioni di rete. Gli amministratori possono specificare l'accesso degli utenti ai protocolli FTP, HTTP, SMTP e Telnet, alla messaggistica immediata (ICQ/AOL Instant Messenger, Windows Live Messenger e Windows Messenger, Jabber, IRC, Yahoo! Messenger e Mail.ru Agent), alla Webmail e alle applicazioni delle reti sociali (AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, e Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING).

ContentLock, altra estensione di DeviceLock, estrae e filtra il contenuto dei dati copiati sulle unità rimovibili e sulle periferiche di memorizzazione Plug-and-Play e dei dati trasmessi sulla rete. Gli amministratori possono creare regole per specificare il tipo di contenuto che può essere copiato e trasmesso.

DeviceLock può monitorare le attività degli utenti per un determinato tipo di periferica o di protocollo su un computer locale. Questa funzionalità del software si basa sul contesto di protezione dell’utente e consente di controllare le attività di un utente o di un gruppo di utenti. DeviceLock utilizza il sottosistema standard di registrazione degli eventi e memorizza le informazioni di controllo nel registro eventi di Windows.

DeviceLock supporta il data shadowing, vale a dire l'abilità di eseguire il mirroring di tutti i dati copiati su periferiche di memorizzazione esterna e trasferiti attraverso la rete o le porte seriali e parallele. È possibile memorizzare la copia completa dei file in un database SQL. Lo shadowing dei dati, così come l'auditing, può essere impostato a livello di utente.

La funzione di shadowing dei dati di DeviceLock è compatibile con il National Software Reference Library mantenuto dal National Institute of Standards and

Technology (NIST) e con l' Hashkeeper Database sviluppato e mantenuto dall'U.S. DOJ National Drug Intelligence Center (NDIC).

I dati raccolti da DeviceLock possono essere verificati con i database hash e possono essere utilizzati per l'analisi forense. Un database hash è un archivio di firme digitali di dati conosciuti e tracciabili.

DeviceLock consente inoltre di archiviare in un proprio database le firme digitali dei file critici (sono supportati gli algoritmi hash SHA-1, MD5 e CRC32) per permettere la tracciabilità delle informazioni. Ad esempio, è possibile tracciare in che ora e con quale periferica gli utenti stanno copiando i file firmati digitalmente.

Per informazioni su come utilizzare i database hash con DeviceLock, contattare il nostro supporto tecnico.

Per ulteriori informazioni sui database hash ed il loro utilizzo, visitare il sito Web del National Software Reference Library: http://www.nsrl.nist.gov.

Inoltre, DeviceLock consente di eseguire ricerche di testo tra i file shadow e i registri di controllo memorizzati nel database centralizzato. DeviceLock può riconoscere, indicizzare, cercare e mostrare automaticamente i documenti in numerosi formati, tra cui: Adobe Acrobat (PDF), Ami Pro, archivi (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documenti, fogli elettronici e presentazioni), Quattro Pro, WordPerfect, WordStar e tanti altri ancora.

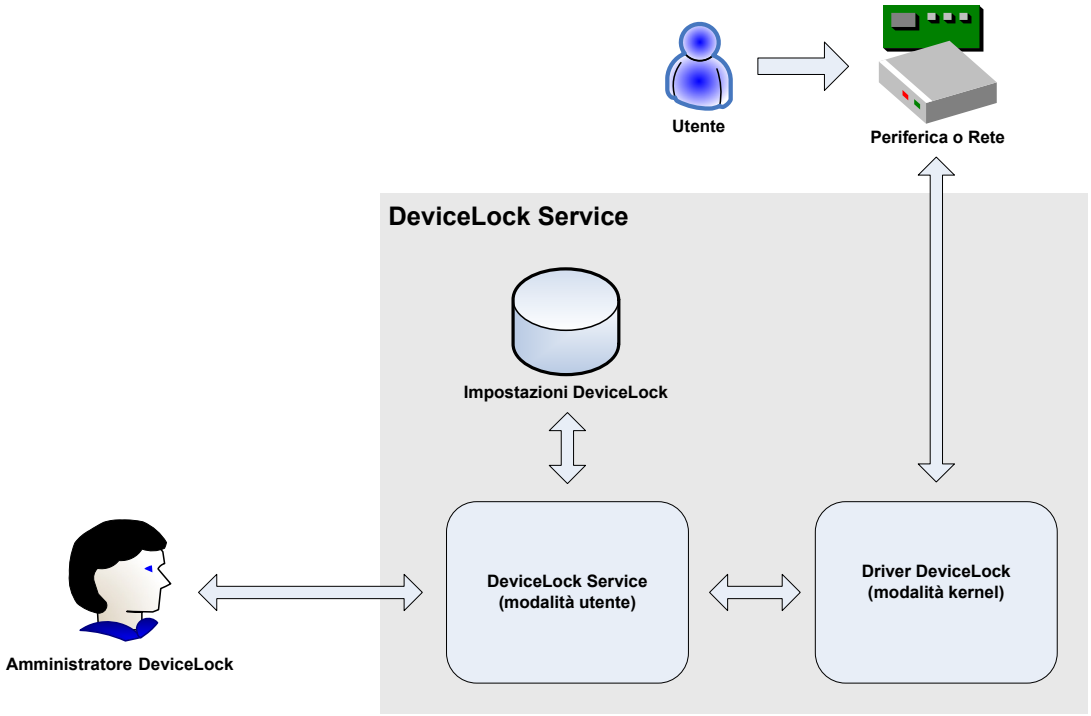
In aggiunta al metodo standard, DeviceLock fornisce un meccanismo più potente per la gestione delle autorizzazioni, ovvero la possibilità di distribuire e cambiare le autorizzazioni e le impostazioni in un dominio Active Directory tramite Criteri di gruppo.

La piena integrazione in Active Directory è una delle funzioni più importanti di DeviceLock e consente agli amministratori di sistema di grandi reti aziendali di gestire e assegnare le autorizzazioni di DeviceLock in modo semplice e comodo.

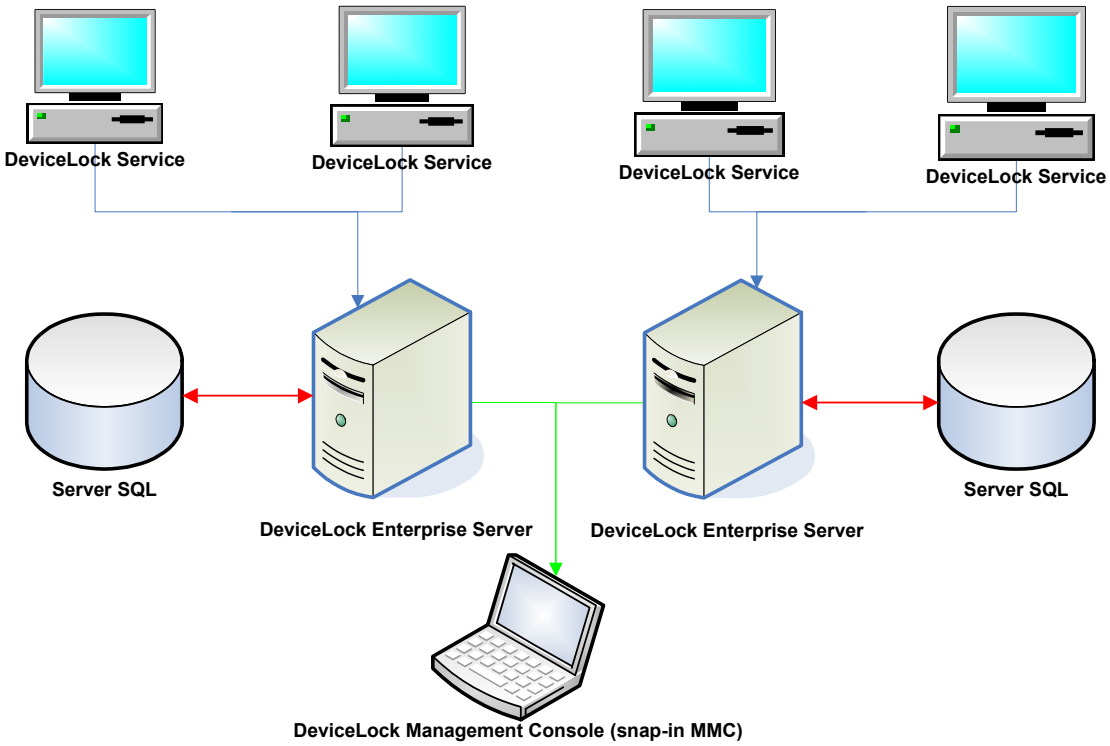
L'integrazione in Active Directory elimina la necessità di installare più applicazioni di terze parti con funzionalità di gestione e distribuzione centralizzata. Per controllare l'intera rete aziendale, DeviceLock utilizza le funzioni standard fornite da Active Directory e non necessita di una propria versione basata su server.

DeviceLock è costituito da tre componenti: un agente (DeviceLock Service), il server (DeviceLock Enterprise Server e DeviceLock Content Security Server) e la console di gestione (DeviceLock Management Console, DeviceLock Group Policy Manager oppure DeviceLock Enterprise Manager).

1. DeviceLock Service costituisce il cuore di DeviceLock. DeviceLock Service è installato su tutti i sistemi client, viene eseguito automaticamente e assicura la protezione delle periferiche e della rete sul computer client, risultando invisibile per gli utenti del computer locale.

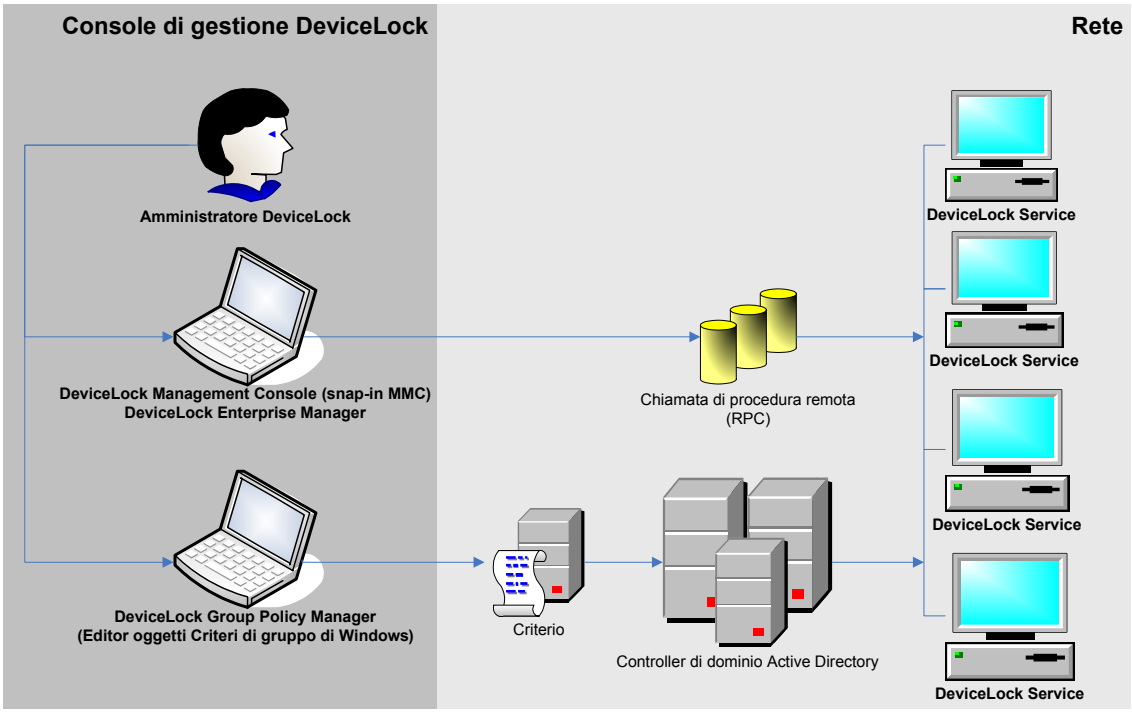


2. DeviceLock Enterprise Server è un componente opzionale che consente la raccolta e l'archiviazione centralizzata delle copie shadow dei dati e dei registri degli eventi di controllo. Per archiviare i propri dati, DeviceLock Enterprise Server utilizza Microsoft SQL Server. Inoltre, è possibile installare DeviceLock Enterprise Server su più macchine per bilanciare meglio il carico di rete.



DeviceLock Content Security Server è un componente opzionale che include DeviceLock Search Server, che consente di eseguire ricerche immediate di testo tra i file shadow e altri registri memorizzati su DeviceLock Enterprise Server. Per ulteriori informazioni, consultare la sezione "Informazioni su DeviceLock Content Security Server".

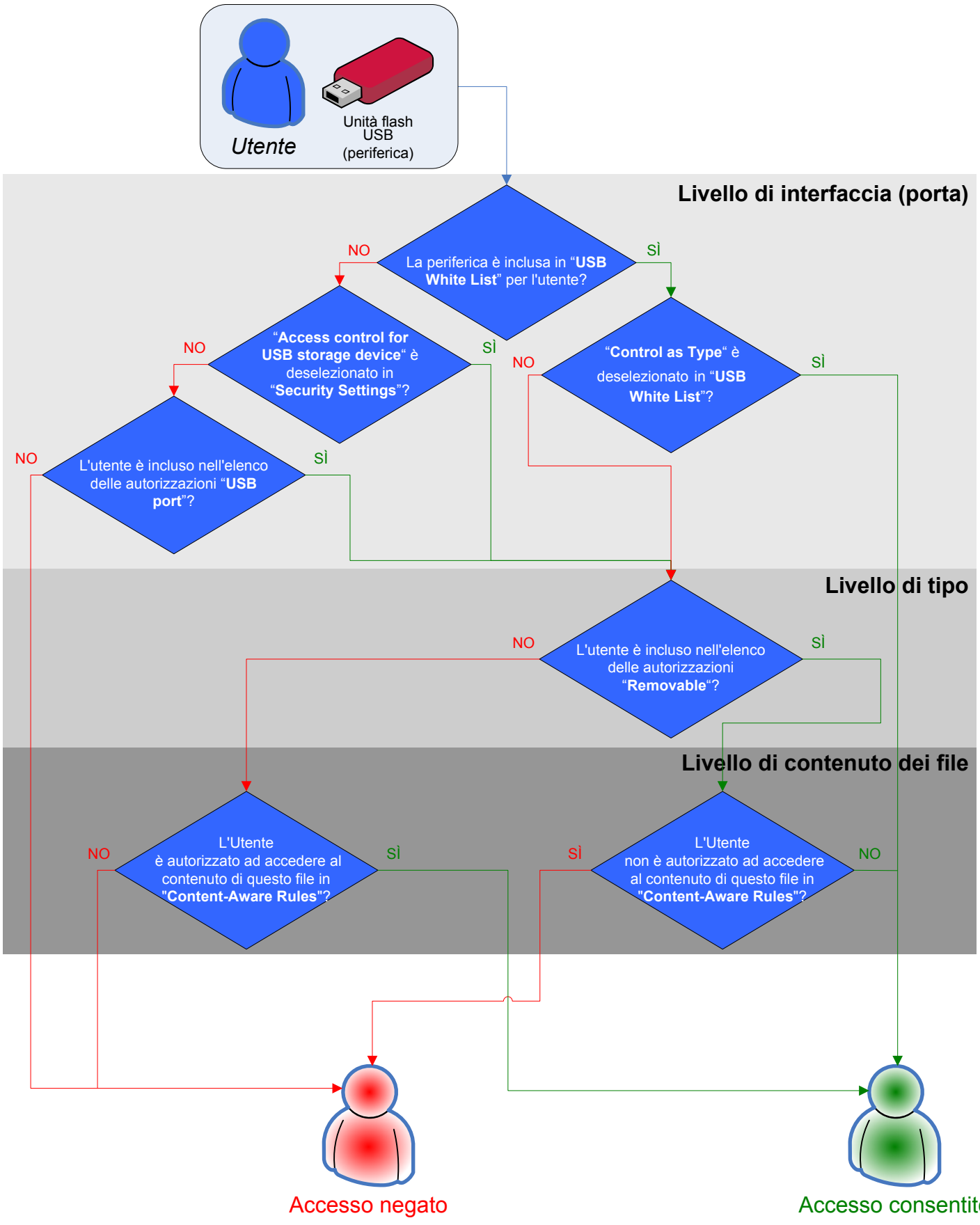
3. La console di gestione è l'interfaccia di controllo che consente agli amministratori di sistema di gestire in remoto i computer sui quali è installato DeviceLock Service. DeviceLock viene distribuito con tre differenti console di gestione: DeviceLock Management Console (snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Group Policy Manager (che si integra nell'Editor oggetti Criteri di gruppo di Windows). DeviceLock Management Console inoltre è utilizzato per gestire DeviceLock Enterprise Server e DeviceLock Content Security Server.



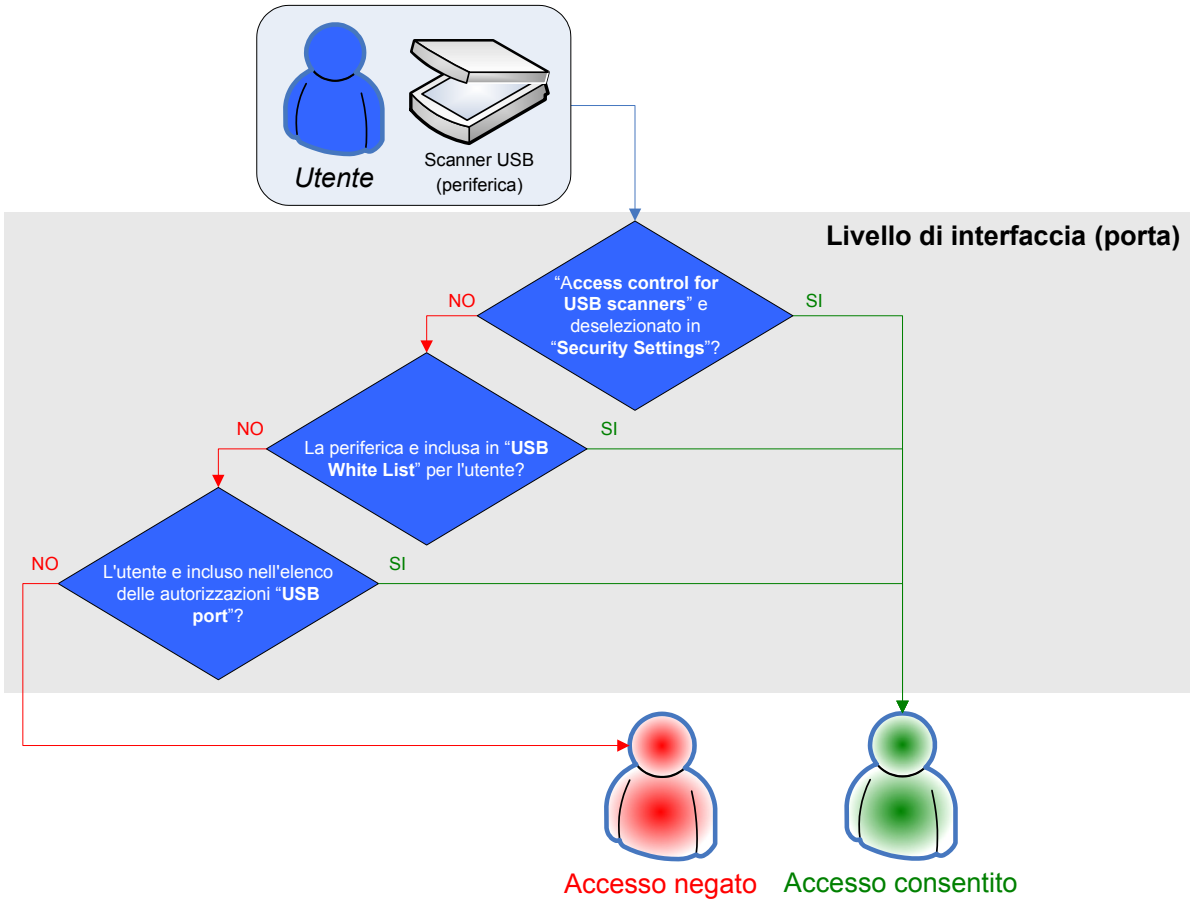
Controllo gestito dell'accesso per periferiche e protocolli

Il controllo dell'accesso per le periferiche funziona nel seguente modo: Ogni qualvolta un utente vuole accedere ad una periferica, DeviceLock intercetta questa richiesta a livello di kernel del sistema operativo. In base al tipo di periferica e al tipo di interfaccia di connessione (ad esempio, USB), DeviceLock verifica i diritti di cui l'utente dispone nell'appropriata ACL (Access Control List - elenco di controllo degli accessi). Se l'utente non dispone dei diritti di accesso necessari per utilizzare la periferica, viene notificato un errore di accesso negato.

Il controllo dell'accesso può avvenire a tre livelli: interfaccia (porta), tipo e contenuto dei file. Per alcune periferiche il controllo viene eseguito per tutti e tre i livelli, per altre per un solo livello, interfaccia (porta) o tipo.


Utente
Unità flash USB (periferica)
Livello di interfaccia (porta)
La periferica è inclusa in "USB White List" per l'utente?
NO
SÌ
"Access control for USB storage device" è deselezionato in "Security Settings"?
NO
SÌ
L'utente è incluso nell'elenco delle autorizzazioni "USB port"?
NO
SÌ
"Control as Type" è deselezionato in "USB White List"?
NO
SÌ
Livello di tipo
L'utente è incluso nell'elenco delle autorizzazioni "Removable"?
NO
SÌ
Livello di contenuto dei file
L'Utente è autorizzato ad accedere al contenuto di questo file in "Content-Aware Rules"?
NO
SÌ
L'Utente non è autorizzato ad accedere al contenuto di questo file in "Content-Aware Rules"?
SÌ
NO
Accesso negato
Accesso consentito

Si ipotizzi che un utente colleghi una unità flash USB ad una porta USB. In questo caso, DeviceLock verifica inizialmente se la porta USB è aperta o bloccata a livello di interfaccia, quindi, successivamente, verifica le autorizzazioni di accesso anche a livello di tipo (unità rimovibile) poiché il sistema operativo riconosce l'unità flash USB come una periferica di archiviazione rimovibile. Inoltre, DeviceLock controlla le autorizzazioni a livello di contenuto dei file (Content-Aware Rules: Regole basate sul contenuto). Uno scanner USB, invece, sarà controllato solo a livello di interfaccia (porta USB), poiché DeviceLock non consente la distinzione degli scanner a livello di tipo.



Sono disponibili ulteriori impostazioni di protezione che consentono di disattivare il controllo di accesso solo per determinate classi di periferica (ad esempio, le stampanti USB). Se una periferica appartiene ad una classe a cui è stato disattivato il controllo di accesso, DeviceLock concederà tutte le richieste di accesso a tale periferica a livello di interfaccia (porta).

DeviceLock supporta inoltre la creazione di particolari white list (white list delle periferiche USB). Grazie a questa funzionalità, è possibile disattivare il controllo di accesso anche solo per determinate periferiche, quali ad esempio le stampanti USB.

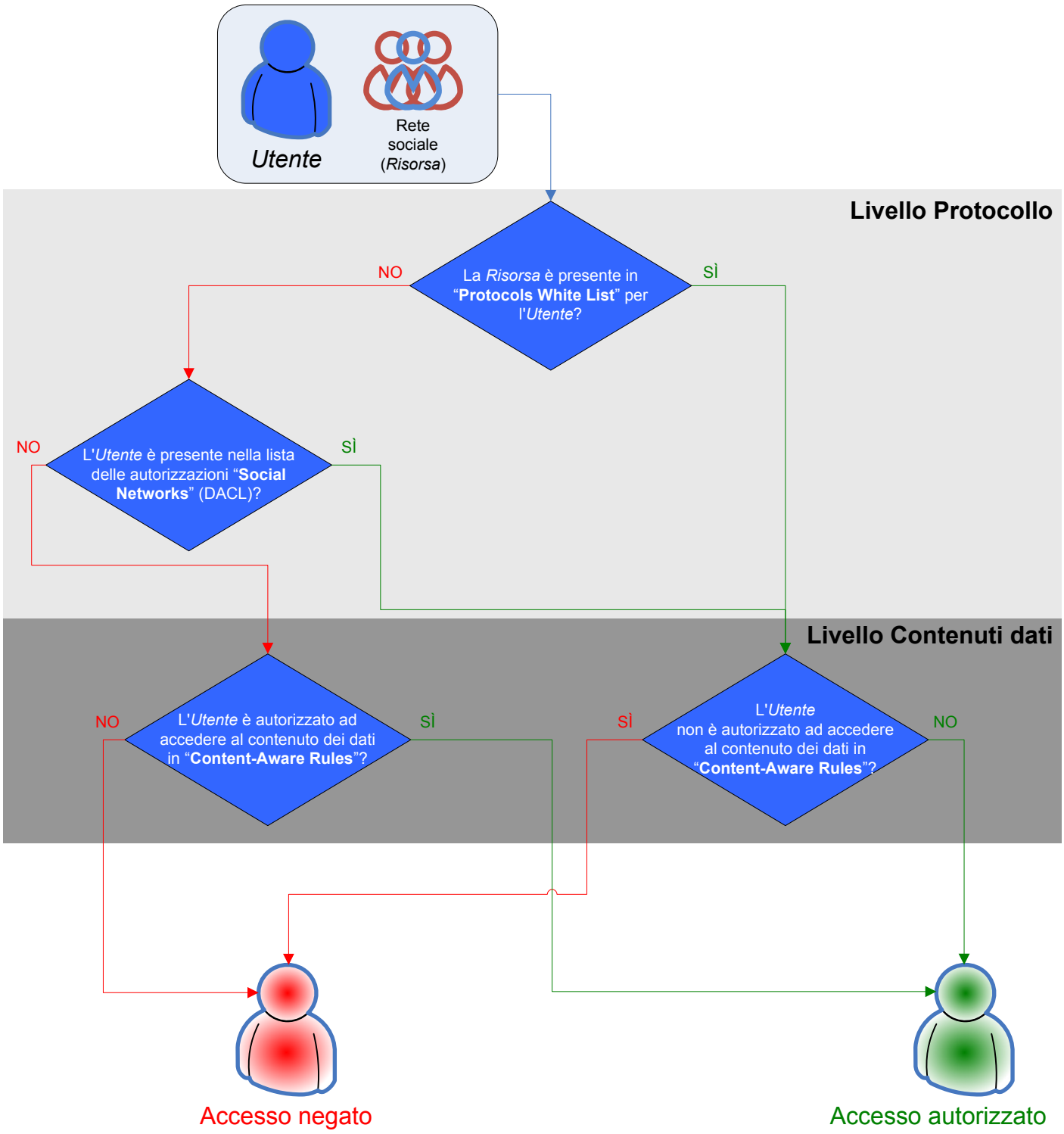
Nota: se l'accesso ad una periferica è negato a livello di interfaccia (porta), DeviceLock non controllerà le autorizzazioni a livello di tipo. Se invece l'accesso è autorizzato a livello di interfaccia (porta), DeviceLock controllerà le autorizzazioni anche a livello di tipo. L'utente può utilizzare una periferica solo quando l'accesso è autorizzato ad entrambi i livelli di controllo.

Il controllo dell'accesso per i protocolli funziona nel seguente modo: ogni volta che un utente tenta di accedere a una risorsa di rete remota, DeviceLock intercetta la richiesta di connessione a livello di kernel del sistema operativo e verifica i diritti dell'utente nell'elenco di controllo di accesso (ACL) pertinente. Se l'utente non ha diritto di accedere al protocollo, viene visualizzato un errore di accesso negato.

Nota: le impostazioni di controllo dell'accesso per le reti sociali e la Webmail hanno la precedenza sulle impostazioni di controllo dell'accesso per l'HTTP. Se, ad esempio, un utente può accedere a Gmail, ma non può utilizzare l'HTTP, potrà comunque accedere al servizio.

Il controllo dell'accesso può avvenire a due livelli: protocollo e contenuto dei dati. Tutte le connessioni di rete (a eccezione delle connessioni Telnet) vengono controllate a entrambi i livelli.

Si consideri il caso di un utente che si collega al sito di una rete sociale. In tal caso, DeviceLock verifica prima se la rete sociale è aperta o bloccata a livello di protocollo. In seguito, DeviceLock verifica le autorizzazioni a livello di contenuto dei dati (Content-Aware Rules: Regole basate sul contenuto).



Inoltre, DeviceLock supporta la creazione di una lista bianca dei protocolli. La lista bianca dei protocolli consente di disattivare il controllo dell'accesso per i collegamenti con determinati parametri (ad esempio le connessioni HTTP a porte e host specifici).

Informazioni su DeviceLock Content Security Server

DeviceLock Content Security Server è un nuovo componente opzionale di DeviceLock. Il componente include Search Server, che consente di eseguire ricerche full-text tra i dati memorizzati in DeviceLock Enterprise Server. Le funzionalità di ricerca consentono di gestire in maniera più facile ed efficiente i dati in continua crescita dei database di DeviceLock Enterprise Server.

DeviceLock Content Security Server include le seguenti funzioni:

- **Supporto della funzionalità di ricerca full-text.** Grazie a Search Server, DeviceLock Content Security Server consente di eseguire ricerche immediate dei dati di testo pertinenti sulla base di diversi criteri.
- **Opzioni di configurazione flessibili.** Sono presenti numerose opzioni di configurazione, che consentono di ottimizzare le prestazioni di DeviceLock Content Security Server in base alle proprie esigenze.

È possibile eseguire ricerche full-text per trovare i dati che normalmente non vengono individuati ricorrendo ai filtri nei visualizzatori di registro. La funzionalità di ricerca full-text è particolarmente utile quando si desidera cercare le copie shadow dei documenti sulla base del loro contenuto.

Use case - Come evitare la perdita di informazioni riservate
Gli specialisti della protezione delle informazioni riservate possono utilizzare regolarmente Search Server per trovare, recuperare e analizzare facilmente tutte le copie shadow dei file contenenti dati business-critical come, ad esempio, gli elenchi di clienti o di prezzi. I record dei registri associati con le copie shadow individuate aiutano a determinare quando e da chi sono state copiate le informazioni riservate. Disponendo di tali informazioni, gli specialisti della protezione possono intraprendere azioni immediate per evitare la divulgazione e la distribuzione dei dati al di fuori dell'azienda.

È possibile configurare e utilizzare DeviceLock Content Security Server utilizzando DeviceLock Management Console.

Funzionamento di Search Server

Search Server presenta le seguenti funzioni:

- Indicizzazione dei dati di DeviceLock Enterprise Server.
- Esecuzione di query full-text in seguito all'indicizzazione dei dati.

Tali funzioni vengono illustrate più nei dettagli di seguito.

Indicizzazione dei dati di DeviceLock Enterprise Server

L'indicizzazione è un processo in seguito al quale i dati di testo presenti in DeviceLock Enterprise Server diventano ricercabili e recuperabili.

Search Server avvia automaticamente il processo di indicizzazione non appena vengono specificati i DeviceLock Enterprise Server. Il risultato del processo di indicizzazione può essere la creazione o l'aggiornamento dell'indice full-text. Poiché è presente un solo indice full-text per Search Server, le attività di gestione risultano più efficienti. L'indice full-text memorizza informazioni sulle parole significative e sulla loro posizione. Durante la creazione o l'aggiornamento dell'indice, Search Server scarta le parole non significative (preposizioni, articoli, ecc.), che non sono rilevanti per le operazioni di ricerca.

Search Server indicizza tutti i dati di testo provenienti dalle seguenti fonti di contenuto: Audit Log, Shadow Log, Deleted Shadow Data Log, Server Log e Monitoring Log.

Il processo di indicizzazione è composto da due fasi. Nella prima fase, Search Server estrae le parole significative dalle copie shadow e dai record di registro e le salva negli indici temporanei per ciascun DeviceLock Enterprise Server specificato. Per ogni indice temporaneo Search Server elabora 1.000 record da ciascun registro.

Nella seconda fase, se il numero di indici temporanei raggiunge 50 o se passano 10 minuti, tutti gli indici temporanei vengono uniti in un indice master permanente che, a sua volta, viene utilizzato per le query di ricerca. Il processo di fusione degli indici temporanei in un indice master viene comunemente chiamato ***merging*** (unione).

Il processo di creazione dell'indice master può richiedere una notevole quantità di tempo. La velocità di indicizzazione può variare in maniera significativa a seconda del tipo di dati indicizzati e dell'hardware utilizzato. In genere, la velocità di indicizzazione va da 30 MB a 120 MB al minuto. Si consideri il seguente esempio:

- Dati: 170 GB, composti da 4.373.004 file di vario genere (HTML, documenti da ufficio, testo)
- Durata dell'indicizzazione: 24,7 ore (6,8 GB/ora)
- Dimensione indice: 12% della dimensione dei documenti originali
- Hardware: Processore Pentium® 4 550 (3,40 GHz, 800 FSB), 2 GB di RAM, unità SATA RAID-0 interne

Esecuzione delle query full-text

Una volta completata l'indicizzazione dei dati di DeviceLock Enterprise Server, è possibile eseguire query full-text. Queste ultime consentono di ricercare una o più parole o frasi specifiche.

Durante una query di ricerca, Search Server elabora la query e recupera un elenco di risultati dall'indice che corrisponde ai criteri della stessa. È possibile applicare filtri alla ricerca per limitare i risultati ottenuti. Ad esempio, i risultati possono essere filtrati in base al registro o alla data.

L'esecuzione di query nell'indice full-text è un'operazione estremamente rapida e flessibile. Un'operazione di ricerca è in grado di rilevare e restituire i risultati corrispondenti a determinati criteri di ricerca in pochi secondi. Per informazioni dettagliate sulla pagina dei risultati della ricerca e sui risultati della ricerca, consultare la sezione "Utilizzo di risultati della ricerca".

Estensione delle funzionalità di DeviceLock con ContentLock e NetworkLock

DeviceLock viene fornito con ContentLock e NetworkLock, componenti concessi in licenza separatamente che aggiungono ulteriori funzionalità a DeviceLock. Questi componenti vengono installati automaticamente ma, per funzionare, devono essere accompagnati dalla rispettiva licenza. Per maggiori informazioni sulle licenze di ContentLock e NetworkLock, consultare la sezione "Licenze."

NetworkLock aggiunge funzionalità complete di controllo contestuale alle comunicazioni di rete a livello di endpoint. Supporta le funzioni di rilevamento e blocco selettivo dei protocolli e delle applicazioni di rete indipendenti dalle porte, la ricostruzione di messaggi e sessioni con estrazione di file, dati e parametri, la registrazione degli eventi e il data shadowing. NetworkLock controlla i protocolli e le applicazioni di rete più comuni: comunicazioni e-mail standard e SMTP con protezione SSL (con verifica separata di messaggi e allegati), accesso al Web e ad altre applicazioni basate su HTTP, inclusa la verifica del contenuto delle sessioni HTTPS crittografate (ad esempio applicazioni di Webmail e di reti sociali come Gmail, Yahoo! Mail, Windows Live Mail, Facebook, Twitter, LiveJournal, ecc.), messaggistica immediata (ICQ/AOL, MSN Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), trasferimento di file su protocolli FTP e FTP-SSL e sessioni Telnet.

NetworkLock viene rappresentato nell'interfaccia utente di DeviceLock Management Console, Service Settings Editor e DeviceLock Group Policy Manager dal nodo **Protocols**.

Caratteristiche e vantaggi principali di NetworkLock:

- **Controllo dell'accesso ai protocolli**. È possibile controllare gli utenti o i gruppi che accedono ai protocolli FTP, HTTP, SMTP e Telnet, alla messaggistica immediata (ICQ/AOL Instant Messenger, Windows Live

Messenger e Windows Messenger, Jabber, IRC, Yahoo! Messenger, Mail.ru Agent), alla Webmail e alle applicazioni delle reti sociali (AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, Yandex Mail; Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING), in base all'ora del giorno e del giorno della settimana.

- **Lista bianca dei protocolli**. Consente di autorizzare in maniera selettiva le comunicazioni di rete su protocolli specifici, indipendentemente dalle impostazioni di blocco dei protocolli esistenti. Questa funzione è particolarmente utile nelle situazioni in cui si dispone di pochi privilegi e in cui viene bloccato tutto il traffico dei protocolli e, in seguito, vengono autorizzati solo i protocolli necessari per l'esecuzione delle normali attività lavorative da parte dei dipendenti.
- **Regole basate sul contenuto (File Type Detection)**. È possibile concedere o negare in maniera selettiva l'accesso a determinati tipi di file trasferiti sulla rete. Il riconoscimento e l'identificazione dei tipi di file si basa unicamente sul contenuto di questi ultimi. Questo algoritmo efficace e affidabile permette di identificare e gestire in maniera corretta i file, indipendentemente dalla loro estensione. Le regole basate sul contenuto (Content-Aware Rules), inoltre, possono essere utilizzate per autorizzare o negare la copia shadow di determinati tipi di file.

  Nota: per utilizzare le funzionalità avanzate delle regole basate sul contenuto, occorre acquistare una licenza di ContentLock.

- **Controllo e shadowing**. Consente di monitorare le attività degli utenti per i protocolli specificati e di registrare una copia completa dei dati/file trasmessi sulla rete.

ContentLock è un componente di monitoraggio e filtraggio che migliora in maniera significativa le prestazioni della funzionalità Content-Aware Rules (Regole basate sul contenuto). ContentLock consente di concedere o negare l'accesso alle informazioni in base ai tipi di file reali e, allo stesso tempo, di creare motivi di espressioni comuni con condizioni numeriche e combinazioni booleane di criteri e parole chiave corrispondenti. ContentLock riconosce oltre ottanta formati di file e tipi di dati e, di conseguenza, è in grado di estrarre e filtrare il contenuto dei dati copiati sulle unità rimovibili e sulle periferiche di memorizzazione Plug-and-Play e dei dati trasmessi sulla rete. ContentLock consente inoltre di filtrare i dati di shadowing per ottenere informazioni utili per la verifica della protezione, le indagini degli incidenti e le analisi "cyber-forensic", prima di salvare i dati nel registro di shadowing. Tale funzionalità consente di ridurre in maniera significativa lo spazio di memorizzazione e i requisiti di larghezza di banda della rete per la consegna del registro di shadowing nel database centrale.

Caratteristiche e vantaggi principali di ContentLock:

- **Controllo dell'accesso ai documenti basato sul contenuto**. È possibile verificare l'accesso ai documenti in base al contenuto di questi ultimi. In tal modo si evita la perdita di contenti riservati e, allo stesso tempo, si permette ai dipendenti autorizzati di accedere alle informazioni necessarie per collaborare.
- **Filtraggio dei dati shadow basato sul contenuto**. È possibile impostare la copia shadow e il salvataggio nel registro di shadowing solo per le informazioni riservate, riducendo in tal modo il volume dei dati del registro e semplificando l'utilizzo dei file di registro.
- **Compatibile con numerosi formati di file e tipi di dati**. È possibile proteggere il contenuto dei seguenti formati di file e tipi di dati: Adobe Acrobat (.pdf), Adobe Framemaker MIF (.mif), Ami Pro (.sam), testo Ansi (.txt), testo SCII, file multimediali ASF (solo metadati) (.asf), CSV (valori separati da virgola) (.csv), DBF (.dbf), EBCDIC, file EML (messaggi e-mail salvati da Outlook Express) (.eml), Enhanced Metafile Format (.emf), file di messaggi Eudora MBX (.mbx), Flash (.swf), GZIP (.gz), HTML (.htm, .html), JPEG (.jpg), Lotus 1-2-3 (.123, .wk?), archivi di e-mail MBOX (incluso Thunderbird) (.mbx), archivi MHT (archivi HTML salvati da Internet Explorer) (.mht), messaggi MIME, file MSG (messaggi e-mail salvati da Outlook) (.msg), file Microsoft Access MDB (.mdb, .accdb, inclusi Access 2007 e Access 2010), Microsoft Document Imaging (.mdi), Microsoft Excel (.xls), Microsoft Excel 2003 XML (.xml), Microsoft Excel 2007 and 2010 (.xlsx), messaggi, note, contatti, appuntamenti e attività di Microsoft Outlook/Exchange, archivi di messaggi di Microsoft Outlook Express 5 e 6 (.dbx), Microsoft PowerPoint (.ppt), Microsoft PowerPoint 2007 e 2010 (.pptx), Microsoft Rich Text Format (.rtf), Tiff ricercabili Microsoft (.tiff), Microsoft Word per DOS (.doc), Microsoft Word per Windows (.doc), Microsoft Word 2003 XML (.xml), Microsoft Word 2007 e 2010 (.docx), Microsoft Works (.wks), MP3 (solo metadati) (.mp3), Multimate Advantage II (.dox), Multimate versione 4 (.doc), documenti, fogli di calcolo e presentazioni OpenOffice versioni 1, 2 e 3 (.sxc, .sxd, .sxi, .sxw, .sxg, .stc, .sti, .stw, .stm, .odt, .ott, .odg, .otg, .odp, .otp, .ods, .ots, .odf) (include il formato di documento aperto OASIS per applicazioni Office), Quattro Pro (.wb1, .wb2, .wb3, .qpw), QuickTime (.mov, .m4a, .m4v), TAR (.tar), TIFF (.tif), TNEF (file winmail.dat), file Treepad HJT (.hjt), Unicode (UCS16, ordine di byte Mac o Windows o UTF-8), file Visio XML (.vdx), Windows Metafile Format (.wmf), file multimediali WMA (solo metadati) (.wma), file video WMV (solo metadati) (.wmv), WordPerfect 4.2 (.wpd, .wpf), WordPerfect (5.0 e versioni successive) (.wpd, .wpf), WordStar versioni 1, 2, 3 (.ws), WordStar versioni 4, 5, 6 (.ws), WordStar 2000, Write (.wri), XBase (inclusi FoxPro, dBase e altri formati compatibili con XBase) (.dbf), XML (.xml), XML Paper Specification (.xps), XSL, XyWrite, ZIP (.zip).
- **Protezione automatica dei nuovi documenti**. È possibile applicare criteri di protezione basati sul contenuto ai nuovi documenti al momento della loro creazione.

- **Diversi metodi di rilevamento del contenuto**. È possibile ricorrere a diversi metodi per identificare il contenuto riservato dei documenti, in base a espressioni comuni, parole chiave e proprietà dei documenti.
- **Gestione del contenuto centralizzata**. Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto, che consentono di definire centralmente i tipi di contenuto per cui verificare l'accesso.
- **Possibilità di sostituire i criteri a livello di tipo di periferica/protocollo**. È possibile concedere o negare in maniera selettiva l'accesso a determinati contenuti, indipendentemente dalle autorizzazioni prestabilite a livello di tipo di periferica/protocollo.
- **Ispezione di file all'interno di archivi**. Consente di effettuare un'ispezione approfondita di tutti i file di un archivio. L'algoritmo utilizzato funziona nel seguente modo: quando un utente cerca di copiare un file di archivio su una periferica o di trasferirlo sulla rete, tutti i file dell'archivio vengono estratti e analizzati separatamente per rilevare il contenuto a cui non è possibile accedere in base alle regole basate sul contenuto (Content-Aware Rules). Se le regole basate sul contenuto negano l'accesso ad almeno uno dei file estratti dall'archivio, l'utente non può accedere a quest'ultimo. Se le regole basate sul contenuto consentono l'accesso a tutti i file estratti dall'archivio, l'utente può accedere a quest'ultimo. Tutti i file archiviati vengono estratti nella cartella Temp del sistema dell'utente. In genere la cartella di sistema Temp si trova nel seguente percorso: directory %windir%\Temp. Se DeviceLock Service non può accedere alla cartella Temp, i file archiviati non vengono analizzati e l'accesso all'archivio viene negato solo se si verifica una delle seguenti condizioni:
  - È presente una regola basata sul contenuto Deny (Nega)
  - Le autorizzazioni impostate per il tipo di periferica o il protocollo negano l'accesso

  Tutti gli archivi nidificati vengono decompressi e analizzati uno a uno. I file di archivio vengono rilevati in base al contenuto e non all'estensione. Sono supportati i seguenti formati di archivio: 7z (.7z); ZIP (.zip); GZIP (.gz, .gzip, .tgz); BZIP2 (.bz2, .bzip2, .tbz2, .tbz); TAR (.tar); LZMA (.lzma); RAR (.rar); CAB (.cab); ARJ (.arj); Z (.z, .taz); CPIO (.cpio); RPM (.rpm); DEB (.deb); LZH (.lzh, .lha); CHM (.chm, .chw, .hxs); ISO (.Iso); UDF (.Iso); COMPOUND (.Msi); WIM (.wim, .swm); DMG (.dmg); XAR (.xar); HFS (.hfs); NSIS (.exe). Gli archivi divisi (o a più volumi) e protetti da password non vengono decompressi.
- **Rilevamento di testo nelle immagini**. La tecnologia di rilevamento di testo nelle immagini consente di classificare le immagini in due gruppi: immagini testuali (ad esempio documenti sottoposti a scansione e schermate di documenti) e immagini non testuali (che non contengono testo). Tale distinzione consente di controllare l'accesso a ciascun gruppo separatamente. Ad esempio, è possibile autorizzare alcuni utenti a copiare immagini non testuali sulle periferiche, ma impedire loro di scrivere immagini testuali,

prevenendo in tal modo la perdita di informazioni riservate contenuti all'interno dei file di immagine. Sono supportati i seguenti file di immagine: file BMP; file Dr. Halo CUT; file DDS; file EXR; file Raw Fax G3; file GIF; file HDR; file ICO; file IFF (tranne file Maya IFF); file JBIG; file JNG; file JPEG/JIF; formato di file JPEG-2000; codestream JPEG-2000; file KOALA; file Kodak PhotoCD; file MNG; file PCX; file PBM/PGM/PPM; file PFM; filePNG; file Macintosh PICT; file Photoshop PSD; file fotocamera RAW; file Sun RAS; file SGI; file TARGA; file TIFF; file WBMP; file XBM; file XPM.

- **Ispezione di immagini incorporate ai documenti**. Consente di eseguire un'ispezione approfondita di tutte le immagini incorporate nei file Portable Document Format (PDF) di Adobe e nei documenti Rich Text Format (RTF) e Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx). Tutte le immagini incorporate vengono estratte dai documenti nella cartella Temp del sistema dell'utente e analizzate indipendentemente dal testo, al fine di rilevare il contenuto a cui non è possibile accedere in base alle regole basate sul contenuto (Content-Aware Rules). Il testo dei documenti viene verificato dalle regole basate sul contenuto create in base ai gruppi di contenuto Keywords (Parole chiave), Pattern (Motivi) o Complex (Complessi). Le immagini incorporate nei documenti vengono verificate dalle regole basate sul contenuto create in base ai gruppi di contenuto File Type Detection (Rilevamento tipo file), Document Properties (Proprietà documenti) o Complex (Complessi). L'accesso ai documenti viene concesso solo se le regole basate sul contenuto autorizzano l'accesso al testo e a tutte le immagini contenuti nei documenti.

Licenze

Per utilizzare le funzionalità di NetworkLock e ContentLock, è necessario acquistare le licenze di NetworkLock e ContentLock, oltre alle licenze di base di DeviceLock. La licenza di NetworkLock consente di utilizzare la funzionalità dei protocolli. La licenza di ContentLock consente di creare e utilizzare regole basate su espressioni comuni, parole chiave e proprietà dei documenti e regole complesse basate sulle combinazioni booleane di criteri corrispondenti.

In caso di utilizzo di diversi tipi di licenza, considerare quanto segue:

- Se si dispone di una licenza di base di DeviceLock, di una licenza di ContentLock e di una licenza di NetworkLock, è possibile utilizzare la funzionalità dei protocolli e creare e utilizzare regole basate su tipi di file, espressioni comuni, parole chiave e proprietà dei documenti e regole complesse.
- Se si dispone unicamente di una licenza di base di DeviceLock, non è possibile utilizzare la funzionalità dei protocolli né creare e utilizzare regole basate su espressioni comuni, parole chiave e proprietà dei documenti e regole

complesse. È possibile creare e utilizzare regole basate sui tipi di file (File Type Detection).

- Se si dispone di una licenza di base di DeviceLock e di una licenza di ContentLock, è possibile creare e utilizzare regole basate su tipi di file, espressioni comuni, parole chiave e proprietà dei documenti e regole complesse. Non è possibile utilizzare la funzionalità dei protocolli.
- Se si dispone di una licenza di base di DeviceLock e di una licenza di NetworkLock, è possibile utilizzare la funzionalità dei protocolli e creare e utilizzare regole basate sui tipi di file. Non è possibile creare regole basate su espressioni comuni, parole chiave e proprietà dei documenti né regole complesse.
- È necessario disporre della licenza di DeviceLock, mentre le licenze di NetworkLock e ContentLock sono opzionali. In caso di assenza della licenza di base o se quest'ultima non è valida, DeviceLock viene eseguito in modalità di prova. Il numero delle licenze di NetworkLock e/o ContentLock deve essere uguale o superiore a quello delle licenze di base di DeviceLock.
- Il periodo di prova di ContentLock e NetworkLock è di 30 giorni.

Misure di protezione di base consigliate

Sono riportate di seguito una serie di procedure di protezione di base che dovrebbero essere adottate sui computer che si desiderano installare in una rete aziendale.

- ***Modificare la sequenza di avvio.*** Il disco rigido deve essere impostato come prima unità di avvio. Modificare la sequenza di avvio nel BIOS, in modo da impedire al computer l'avvio da unità floppy, unità USB o unità CD-ROM. Se non si modifica la sequenza di avvio scegliendo come prima opzione l'unità disco rigido, è possibile utilizzare un CD avviabile o una unità flash USB per accedere direttamente all'unità disco rigido.
- ***Proteggere il BIOS con una password.*** Impostare la password BIOS per impedire a utenti non autorizzati l’accesso alle impostazioni del BIOS. Se il BIOS non è protetto da password, è possibile modificare la sequenza di avvio e utilizzare un CD avviabile, un disco floppy o una unità flash USB (v. procedura precedente).
- ***Sigillare il telaio dei computer.*** Proteggere l'hardware con un sigillo. In caso contrario, sarà possibile collegare un'unità di avvio esterna direttamente al computer e accedere al disco rigido. Inoltre, se si riesce ad accedere fisicamente alla scheda madre, è relativamente semplice individuare il jumper di reset CMOS e cancellare la password BIOS (v. procedura precedente).
- ***Non concedere privilegi di amministratore a utenti standard.*** Gli utenti standard non dovrebbero essere membri del gruppo locale Administrators. Non è buona norma concedere agli utenti privilegi amministrativi sui propri computer.

Se, per qualche motivo, gli utenti della rete dispongono di privilegi amministrativi sui propri computer, DeviceLock fornisce un ulteriore livello di protezione. Nessun utente, ad eccezione degli amministratori autorizzati di DeviceLock, è in grado di connettersi a DeviceLock Service, di interromperlo o di disinstallarlo. Perfino i membri del gruppo locale Administrators non sono in grado di disattivare DeviceLock se non sono presenti nell'elenco degli amministratori autorizzati di DeviceLock.

- ***Rimuovere la console di ripristino di emergenza.*** Se la console di ripristino di Windows è installata sul computer locale, è possibile avviare il computer in modalità di ripristino e aggirare le misure di protezione, inclusa la disabilitazione di DeviceLock Service (questa operazione richiede comunque l'inserimento della password dell'amministratore locale). Per questo motivo, si consiglia di eliminare la console di ripristino di emergenza. Per ulteriori informazioni sulle operazioni da effettuare per installare, rimuovere e utilizzare la console di ripristino, consultare il seguente articolo online di Microsoft: http://support.microsoft.com/kb/307654/it.

Installazione

Richieste di sistema

DeviceLock Manager può essere installato su qualsiasi computer che esegue Windows NT 4.0 SP6, Windows 2000, Windows XP/Vista/7 e Windows Server 2003/2008. Supporta le piattaforme a 32 e 64 bit. Sui computer con sistema operativo Windows NT 4.0 SP 6 deve essere installato Microsoft Internet Explorer 4.0 o versioni successive.

Nota: NetworkLock incluso in DeviceLock non è compatibile con il sistema operativo Windows NT 4.0 SP 6.

Per installare ed utilizzare DeviceLock, è necessario disporre dei privilegi di amministratore. Per utilizzare DeviceLock su un computer locale, è necessario disporre di privilegi amministrativi su tale computer. Per utilizzare DeviceLock in un ambiente di rete, è necessario disporre di privilegi amministrativi sul dominio di rete.

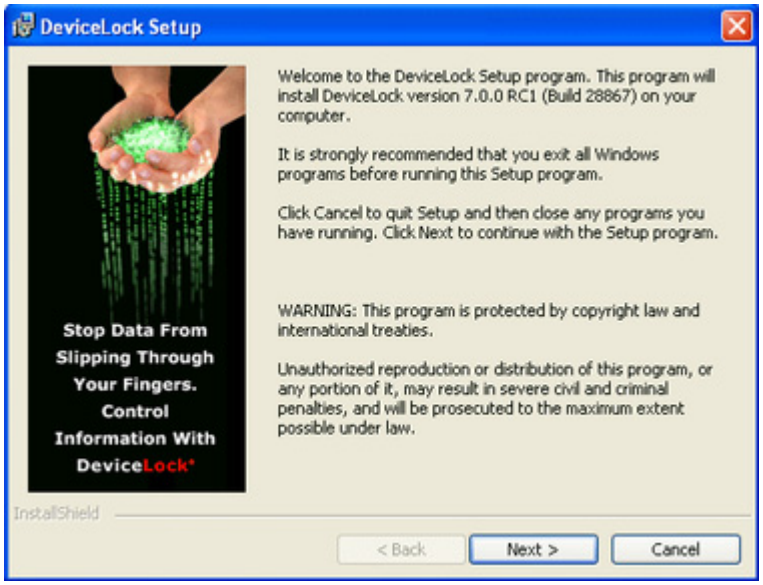
Se si desidera utilizzare DeviceLock in un ambiente di rete, assicurarsi che sia attivo il protocollo di rete TCP/IP. DeviceLock può essere utilizzato anche su computer stand-alone. Un ambiente di rete è necessario solamente se si desidera gestire DeviceLock Service da un computer remoto.

Distribuzione di DeviceLock Service

È necessario installare DeviceLock Service sui computer su cui effettuare il controllo dell'accesso alle periferiche collegate. È possibile distribuire DeviceLock Service sui sistemi client in più modi differenti.

Installazione interattiva

Avviare il programma di installazione (**setup.exe**) e seguire le istruzioni visualizzate sullo schermo.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

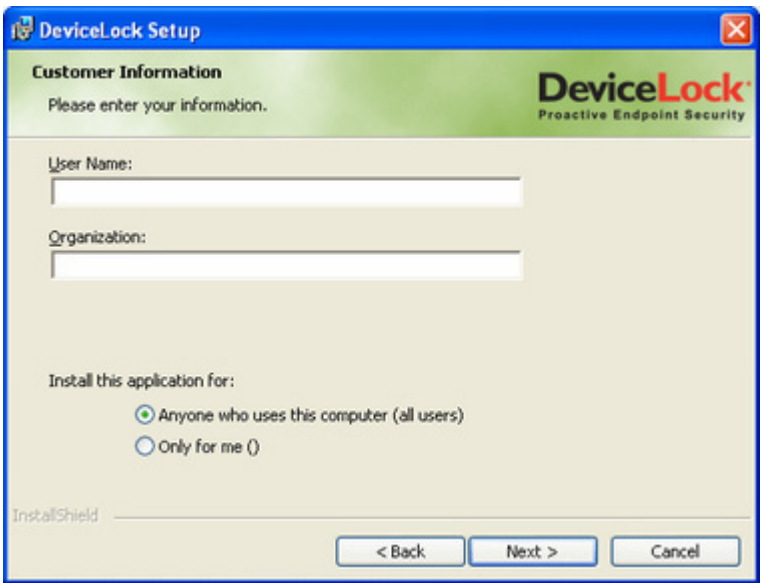
Eseguire il programma di installazione **setup.exe** su ciascuno dei computer che si desidera controllare con DeviceLock Service.

Se si sta aggiornando una versione precedente di DeviceLock Service, assicurarsi di disporre dei privilegi di amministratore di DeviceLock Service. In caso contrario, non sarà possibile continuare l'installazione.

Per proseguire con l'installazione, è necessario accettare le clausole del Contratto di licenza con l'utente finale.

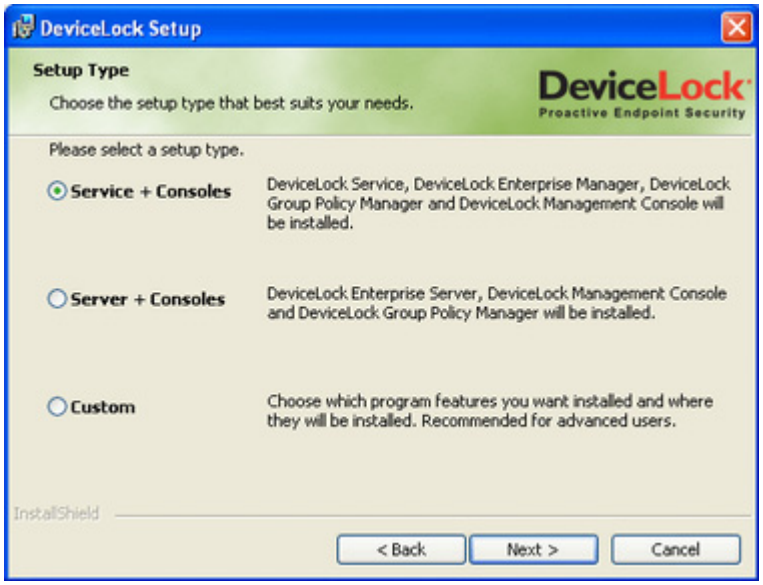
Nella pagina **Customer Information**, digitare il proprio nome utente e il nome dell'organizzazione. Nella stessa pagina, nella sezione **Install this application for** è possibile specificare i collegamenti sul desktop da creare per le console di gestione di DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager e DeviceLock Service Settings Editor). È possibile selezionare una delle seguenti opzioni:

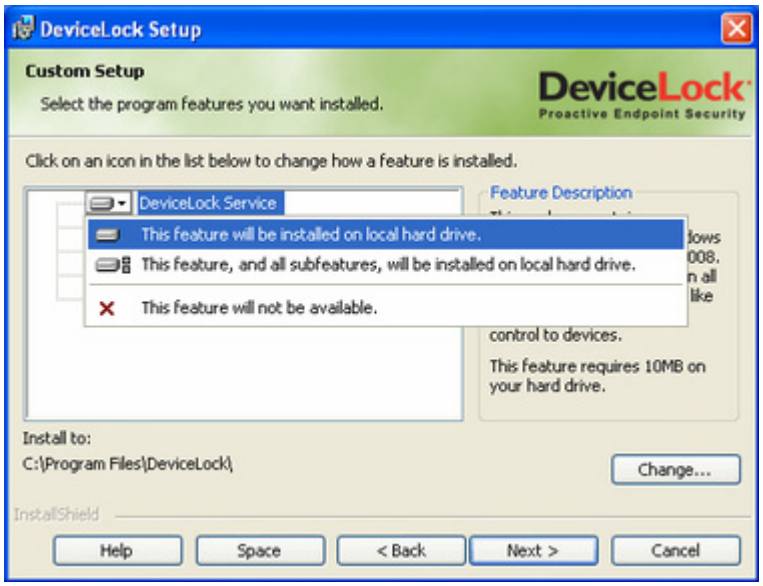
- **Anyone who uses this computer (all users)**: crea collegamenti sul desktop sulle console di gestione di DeviceLock per tutti gli utenti.
- **Only for me**: crea collegamenti sul desktop sulle console di gestione di DeviceLock solo per l'account che sta installando DeviceLock.



Nella pagina **Setup type**, selezionare il tipo di installazione desiderata.

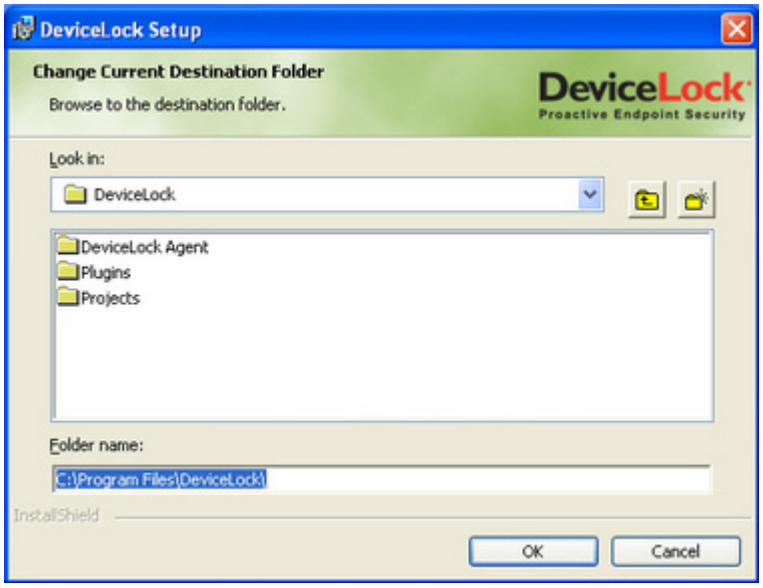
Sono disponibili due opzioni: per installare sia DeviceLock Service sia le console di gestione di DeviceLock, selezionare **Service + Consoles**; per installare unicamente DeviceLock Service, selezionare **Custom** e scegliere il componente **DeviceLock Service**.


DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

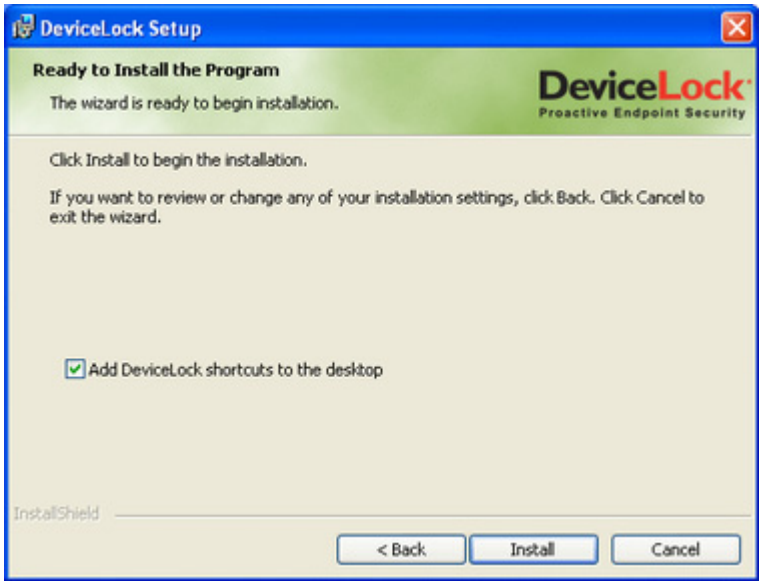

DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
Feature Description
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
control to devices.
This feature requires 10MB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

Nota: nella pagina **Custom Setup** è possibile selezionare il componente RSoP (Resultant Set of Policy: Gruppo di criteri risultante) da installare. Quest'ultimo attiva il supporto della modalità di pianificazione RSoP di DeviceLock sui controller di dominio. Il componente RSoP è richiesto unicamente quando sul computer in uso sono installate le console di gestione DeviceLock, mentre DeviceLock Service non è installato. Per ulteriori informazioni sulla modalità di pianificazione RSoP, consultare la documentazione di Microsoft.

Nella pagina **Custom Setup** è possibile modificare le directory di installazione predefinita. La directory di installazione predefinita di DeviceLock è **%ProgramFiles%\DeviceLock**. Per modificare la directory di installazione predefinita, fare clic su **Change** per aprire la pagina **Change Current Destination Folder**.



Nella pagina **Ready to Install the Program**, fare clic su **Install** per avviare l'installazione. Selezionare la casella di controllo **Add DeviceLock shortcuts to the desktop** per aggiungere i collegamenti a DeviceLock Management Console (lo snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Service Settings Editor sul desktop.

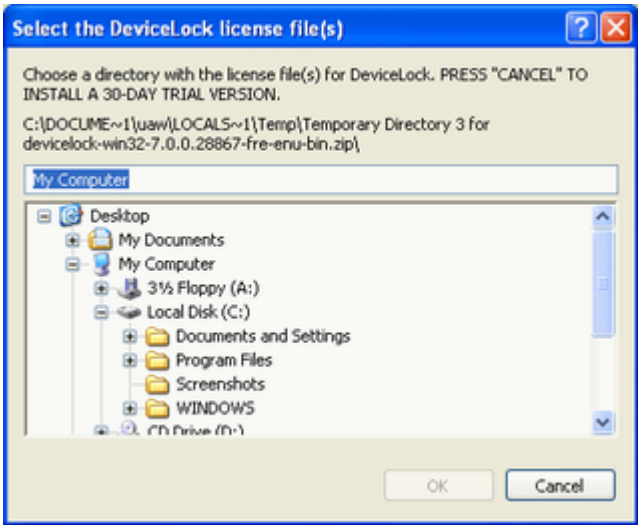

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Qualora si sia scelto di installare anche le console di gestione di DeviceLock, il programma di installazione chiederà di creare un nuovo certificato di DeviceLock.

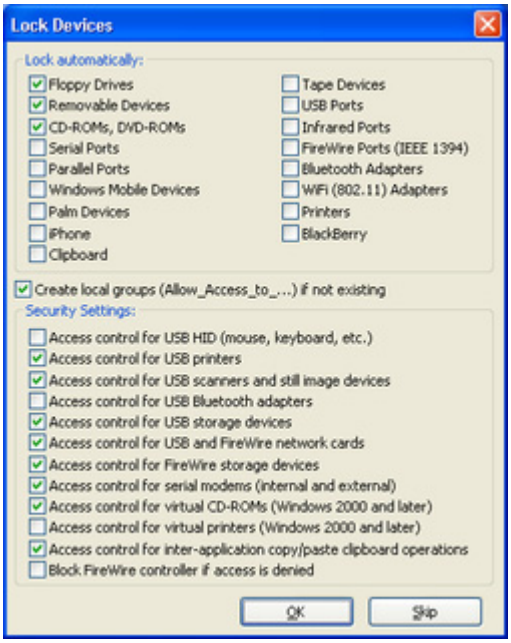
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

È possibile creare un nuovo certificato di DeviceLock anche successivamente, utilizzando lo strumento di generazione dei certificati installato assieme alle console di gestione di DeviceLock. Quindi, in caso di dubbio, fare clic sul pulsante **No** e continuare l'installazione. Per ulteriori informazioni sui certificati di DeviceLock, consultare la sezione "Certificati di DeviceLock".

Se viene selezionata l'opzione **Service + Consoles**, potrebbe essere visualizzato un messaggio in cui si richiede il caricamento dei file di licenza di DeviceLock. Se non si dispone di file di licenza, fare clic su **Cancel** per installare una versione di prova di 30 giorni di DeviceLock.



Durante la fase di installazione, è possibile assegnare speciali autorizzazioni alle periferiche locali.



Selezionare le periferiche a cui applicare le autorizzazioni. Se si seleziona la casella di controllo **Create local groups if not existing**, il programma d'installazione creerà il gruppo speciale di utenti locali Allow_Access_To_ (uno per ogni tipo di periferica selezionata) se questo non è presente sul computer locale. Ad esempio, se si seleziona la casella di controllo Floppy Drives, il programma creerà il gruppo di utenti Allow_Access_To_Floppy associato alle unità floppy.

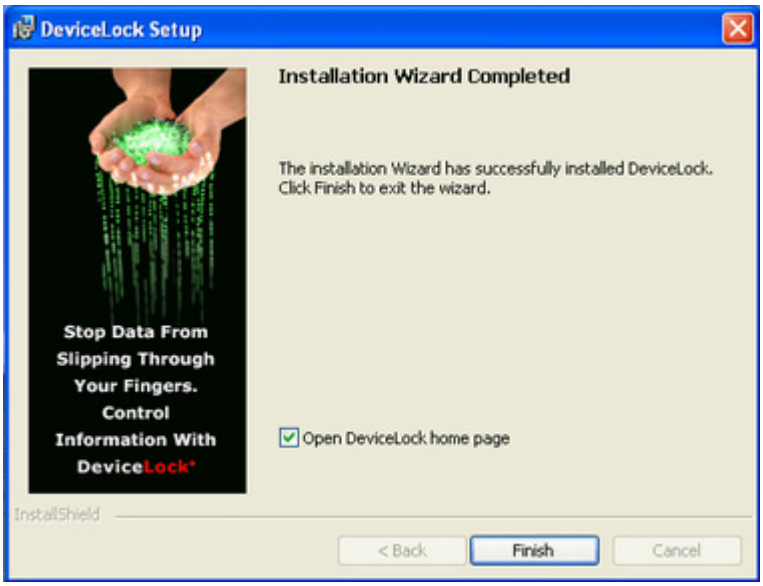
Il programma di installazione assegna diritti generici **Read**, **Write**, **Format** e **Eject** ai membri del gruppo Administrators e all'account SYSTEM. Ai membri del gruppo Allow_Access_To_ sono assegnati i diritti generici **Read**, **Write** e **Eject**.

Inoltre, è possibile configurare le impostazioni di protezione per disattivare il controllo di accesso per determinati tipi di periferica.

Se si selezionano le caselle di controllo **Access control for USB HID**, **Access control for USB printers**, **Access control for USB scanners and still image devices**, **Access control for USB Bluetooth adapters**, **Access control for USB storage devices** oppure **Access control for FireWire storage devices**, DeviceLock Service attiverà il controllare di accesso per le periferiche di input HID (mouse e tastiera), stampanti, scanner, adattatori Bluetooth o periferiche di archiviazione (quali le unità flash) collegate alle porte USB e FireWire. Per attivare il controllo di accesso per le schede di rete USB e FireWire, selezionare la casella di controllo **Access control for USB and FireWire network cards**. Se si sceglie di non selezionare queste caselle di controllo, le periferiche installate continueranno a funzionare regolarmente, anche se collegate a porte USB e/o FireWire bloccate. Per attivare il controllo di accesso per i modem seriali (interni e/o esterni), selezionare la casella di controllo **Access control for serial modems**. Per sbloccare le unità virtuali CD-ROM (emulate via software) sui sistemi Windows 2000 e versioni successive, deselezionare la casella di controllo **Access control for virtual CD-ROMs**. Per sbloccare il controllo delle stampanti virtuali (quelle che stampano su file) su Windows 2000 e sistemi successivi, deselezionare la casella di controllo **Access control for virtual printers**. Per attivare il controllo dell'acceso per le operazioni di copia/incolla degli Appunti tra diverse applicazioni, selezionare la casella di controllo **Access control for inter-application copy/paste clipboard operations**. In caso contrario, anche se gli Appunti sono bloccati, il controllo dell'accesso per le operazioni di copia/incolla tra diverse applicazioni risulta disattivato. Per disattivare i controller FireWire quando l’account Everyone dispone delle autorizzazioni No Access per il tipo di periferica porta FireWire, selezionare la casella di controllo **Block FireWire controller if access is denied**.

Per applicare le modifiche, fare clic sul pulsante **OK**. Se si preferisce applicare le autorizzazioni alle periferiche al termine dell'installazione di DeviceLock, fare clic sul pulsante **Skip**.

Una volta completata l'installazione del software, il programma di installazione consiglierà di visitare il sito Web di DeviceLock.



Deselezionare la casella di controllo **Open DeviceLock home page** se non si desidera visitare il sito Web di DeviceLock. Fare clic su **Finish** per terminare l'installazione.

Nota: per disinstallare DeviceLock, eseguire una delle seguenti azioni:

Aprire **Installazione applicazioni** nel Pannello di controllo per rimuovere **DeviceLock**.
- OPPURE -
Fare clic su **Start**, selezionare **Tutti i programmi**, **DeviceLock**, quindi fare clic su **Remove DeviceLock**.

Installazione automatica

Il programma di installazione di DeviceLock supporta l'installazione in modalità automatica. Questo consente di eseguire l'installazione del software dall'interno di un file batch. Per installare DeviceLock Service senza richiedere l'intervento dell'utente, avviare il programma d'installazione con il parametro **/s** (ad esempio: **c:\setup.exe /s**). I dati dei parametri per personalizzare le operazioni di installazione in modalità automatica sono recuperabili nel file di configurazione ***devicelock.ini***. Il file devicelock.ini deve essere memorizzato nella stessa cartella in cui è presente il file setup.exe. Grazie a questo file, è possibile personalizzare i parametri di installazione.

È possibile aprire e modificare il file devicelock.ini con qualsiasi editor di file di testo, quale ad esempio Blocco note. Rimuovere il carattere punto e virgola (;) prima di assegnare un valore ad un parametro. Per assegnare ad un parametro il valore predefinito, non rimuovere il carattere punto e virgola.

Il file di configurazione è composto da due sezioni (**[Install]** e **[Misc])** ciascuna delle quali include parametri propri:

1. [Install]

Per installare DeviceLock Service, specificare il parametro **Service**:

Service = 1

Per installare anche le console di gestione di DeviceLock e la documentazione, utilizzare i parametri **Manager** e **Documents**.

Se si desidera solamente aggiornare DeviceLock Service senza modificare le impostazioni esistenti, utilizzare il parametro **OnlyUpgradeService**:

OnlyUpgradeService = 1

In questo caso il programma di installazione ignora tutte le impostazioni specificate e aggiorna unicamente DeviceLock Service alla nuova versione.

È possibile specificare anche in quale cartella installare DeviceLock:

InstallDir = C:\Programmi\DeviceLock

Il programma di installazione utilizzerà la cartella specificata qualora non sia in grado di trovare un'installazione precedente di DeviceLock.

Se sono state acquistate licenze per DeviceLock, è possibile specificare il percorso dei file di licenza:

RegFileDir = *C:\Cartella*

In cui *C:\Cartella* è il percorso che contiene i file di licenza.

Se viene installato unicamente DeviceLock Service, non è necessario caricare le licenze. Le licenze sono necessarie per le console di gestione di DeviceLock e per i componenti con licenza separata (ContentLock e NetworkLock).

Per indicare a DeviceLock Service di utilizzare una porta fissa, specificare il parametro **FixedPort**:

FixedPort = *[numero porta]*

dove *numero porta* rappresenta il numero della porta TCP fissa che DeviceLock Service utilizzerà per comunicare con le console di gestione. Per utilizzare porte dinamiche per la comunicazione RPC, specificare 0 come numero di porta. Per impostazione predefinita, DeviceLock Service utilizza la porta 9132.

Se al parametro **CreateGroups** viene assegnato il valore "1", il programma di installazione creerà il gruppo speciale di utenti locali Allow_Access_To_, se non è già

esistente sul computer locale, per ogni tipo di periferica installata (ad esempio, il gruppo di utenti Allow_Access_To_Floppy sarà associato alle unità floppy).

Per applicare impostazioni, autorizzazioni, regole di controllo e di shadowing a DeviceLock Service, specificare il percorso del file XML precedentemente salvato nel parametro **SettingsFile**:

SettingsFile = C:\settings.dls

Il file delle impostazioni può essere creato utilizzando DeviceLock Management Console, DeviceLock Group Policy Manager e/o DeviceLock Service Settings Editor.

2. [Misc]

Per eseguire un programma (ad esempio, un file batch) al termine dell'installazione, è possibile utilizzare il parametro **Run**:

Run = *C:\ miofilebatch.bat*

Per impedire il riavvio automatico del sistema anche quando viene richiesto dal programma di installazione, impostare il parametro **DisableRestart** su "1".

Installazione tramite Microsoft Systems Management Server

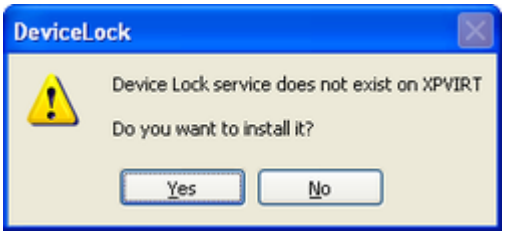
L'installazione automatica consente di distribuire DeviceLock Service tramite Microsoft Systems Management Server (SMS).

Utilizzare i file di definizione del pacchetto (DevLock.pdf per SMS versione 1.x e DevLock.sms per SMS 2.0 e versioni successive) forniti con DeviceLock e memorizzati nell'archivio sms.

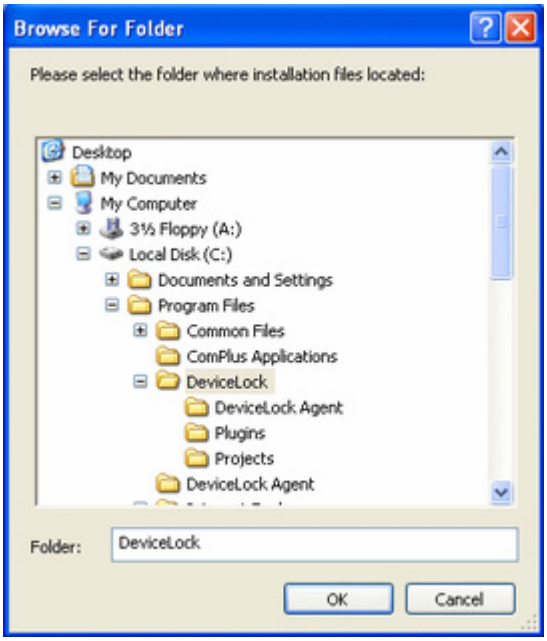
Installazione remota tramite DeviceLock Management Console

DeviceLock Management Console (lo snap-in MMC) supporta l'installazione remota. Questo consente ad un amministratore di sistema di configurare un servizio su una macchina remota senza dover essere fisicamente presente presso il computer.

Quando si effettua la connessione ad un computer, la console di gestione consiglia l'installazione o l'aggiornamento di DeviceLock Service nei casi in cui il servizio non risulti installato o la versione installata risulti obsoleta.



Selezionare la directory che contiene tutti i file necessari per l'installazione (ad esempio DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe e InstMsiW.exe).

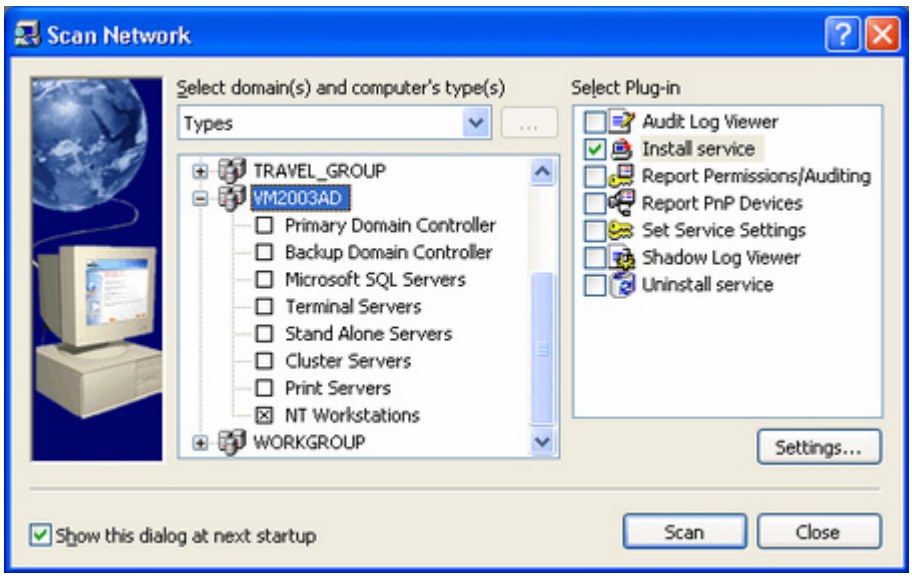


Questi file si trovano nella directory di installazione di DeviceLock. La directory di installazione predefinita di DeviceLock è **%ProgramFiles%\DeviceLock**.

Per impostazione predefinita, i file di installazione di DeviceLock Service vengono copiati nella cartella %ProgramFiles%\DeviceLock Agent se questo servizio non è presente sul sistema in uso. Se il servizio è presente sul sistema in uso ma la versione è inferiore a 7.0, la console di gestione copia anche i file di installazione nella cartella predefinita %ProgramFiles%\DeviceLock Agent. Se il servizio è presente sul sistema in uso ma la versione è 7.0 o superiore, la console di gestione copia i file di installazione nella directory già presente, sostituendo i file precedenti.

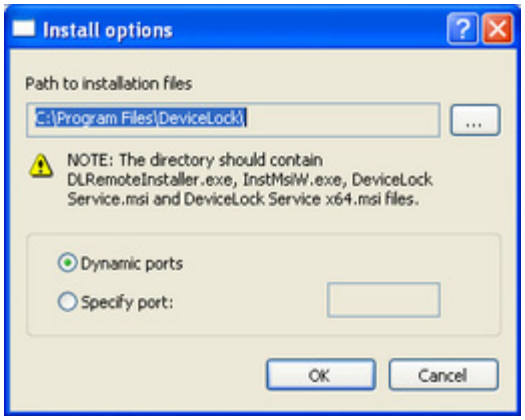
Installazione remota tramite DeviceLock Enterprise Manager

DeviceLock Enterprise Manager include il plug-in Install service che consente di distribuire automaticamente DeviceLock Service su tutti i computer selezionati collegati alla rete aziendale.



Innanzitutto, selezionare i computer sui quali deve essere installato DeviceLock Service. DeviceLock Enterprise Manager consente di selezionare i computer in base al nome e al tipo. È possibile caricare l'elenco dei computer da un file esterno oppure è possibile selezionare i computer da una struttura LDAP (Active Directory, Novell eDirectory, OpenLDAP e così via).

In seguito, selezionare il plug-in **Install service** e fare clic sul pulsante **Settings** per specificare la directory che contiene tutti i file necessari per l'installazione (ad esempio DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe e InstMsiW.exe). Questi file si trovano nella directory di installazione di DeviceLock. La directory di installazione predefinita di DeviceLock è **%ProgramFiles%\DeviceLock**. È possibile specificare a DeviceLock Service di utilizzare una porta TCP fissa per comunicare con le console di gestione. Per utilizzare le porte dinamiche per la comunicazione RPC, selezionare l'opzione **Dynamic ports**. Per impostazione predefinita, DeviceLock Service utilizza la porta 9132.



Per impostazione predefinita, i file di installazione di DeviceLock Service vengono copiati nella cartella %ProgramFiles%\DeviceLock Agent se questo servizio non è presente sul sistema in uso. Se il servizio è presente sul sistema in uso ma la versione è inferiore a 7.0, il plug-in Install service copia anche i file di installazione nella cartella predefinita %ProgramFiles%\DeviceLock Agent. Se il servizio è presente sul sistema in uso ma la versione è 7.0 o superiore, il plug-in Install service copia i file di installazione nella cartella già presente, sostituendo i file precedenti.

Installazione tramite Criteri di gruppo

Le seguenti istruzioni descrivono passo passo come utilizzare Criteri di gruppo per distribuire automaticamente DeviceLock Service sui computer client. DeviceLock Service può essere distribuito in un dominio di Active Directory utilizzando il pacchetto Microsoft Software Installer (DeviceLock Service.msi e DeviceLock Service x64.msi).

Nota: l'installazione automatizzata dei programmi mediante Criteri di gruppo di Windows richiede che sui computer client sia in esecuzione Windows 2000 o versione successiva.

Se si utilizza un pacchetto MSI personalizzato, e DeviceLock Service è impostato in modo da distribuire DeviceLock Service mediante i Criteri di gruppo, queste impostazioni non si applicano ai computer client in presenza di una delle seguenti condizioni:

- L'impostazione di protezione predefinita è disattivata nel DeviceLock Service eseguito da remoto.

- I Criteri di gruppo (GPO) applicati ai computer client hanno l'impostazione **Override Local Policy** attivata.

Per informazioni sulla creazione di un pacchetto MSI personalizzato, consultare la sezione "Create MSI Package."

Per distribuire DeviceLock Service mediante i Criteri di gruppo, seguire i seguenti passaggi:

- **Creazione di un punto di distribuzione**
  Per installare DeviceLock Service, è necessario creare un punto di distribuzione sul server, come illustrato di seguito:
  1. Connettersi al computer server con i privilegi di amministratore.
  2. Creare una cartella di rete condivisa nella quale memorizzare il pacchetto MSI.
  3. Impostare le autorizzazioni di accesso alla cartella in modo da consentire la distribuzione del pacchetto.
  4. Copiare il pacchetto MSI (DeviceLock Service.msi e/o DeviceLock Service x64.msi) nel punto di distribuzione.

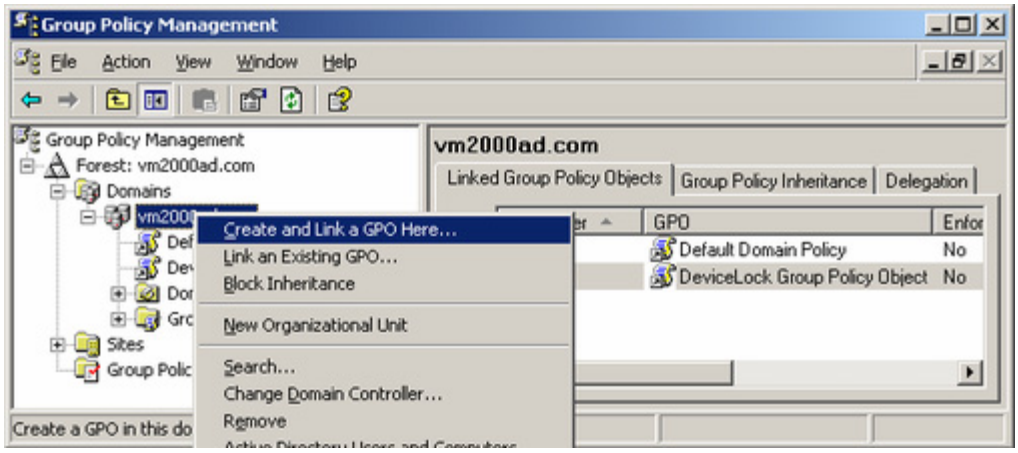
- **Creazione di un oggetto Criteri di gruppo**

  Per creare un oggetto Criteri di gruppo (GPO) da utilizzare per distribuire DeviceLock Service:

  1. Avviare lo snap-in Gestione Criteri di gruppo.

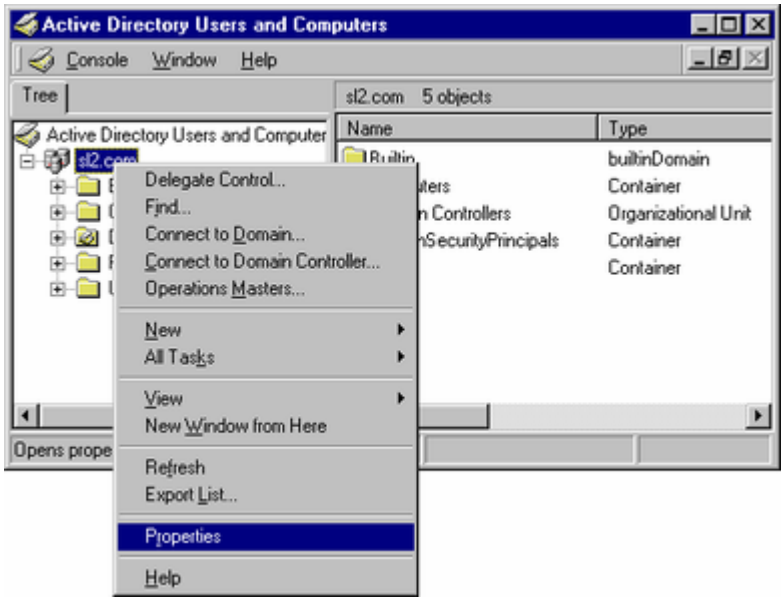
     Se lo snap-in Gestione Criteri di gruppo non è installato sul computer, è possibile utilizzare in alternativa lo snap-in Utenti e computer di Active Directory.

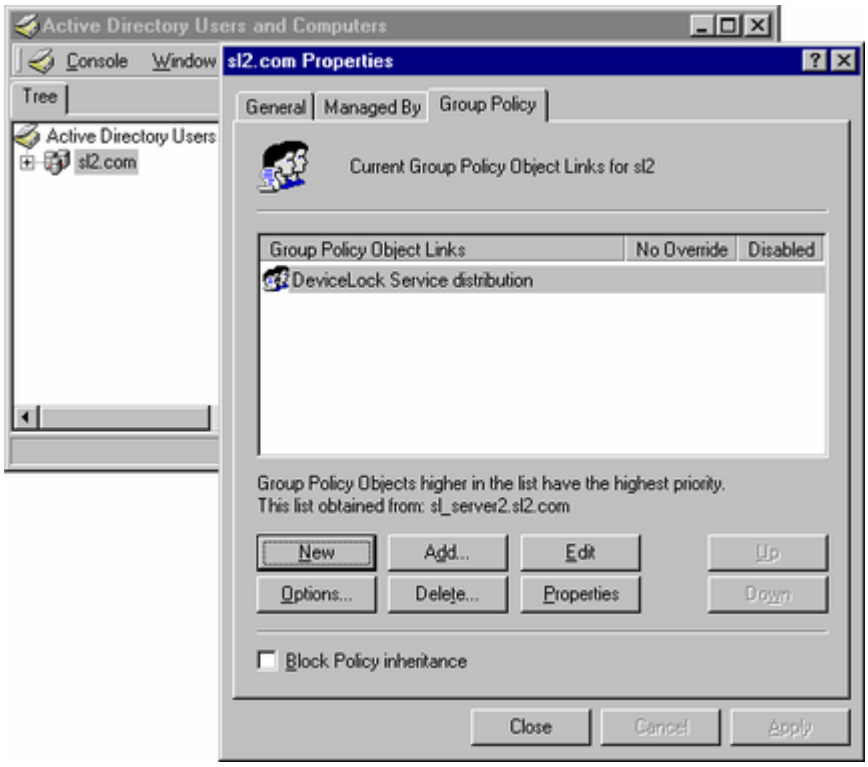
  2. Nella struttura della console, fare clic con il pulsante destro del mouse sul dominio.



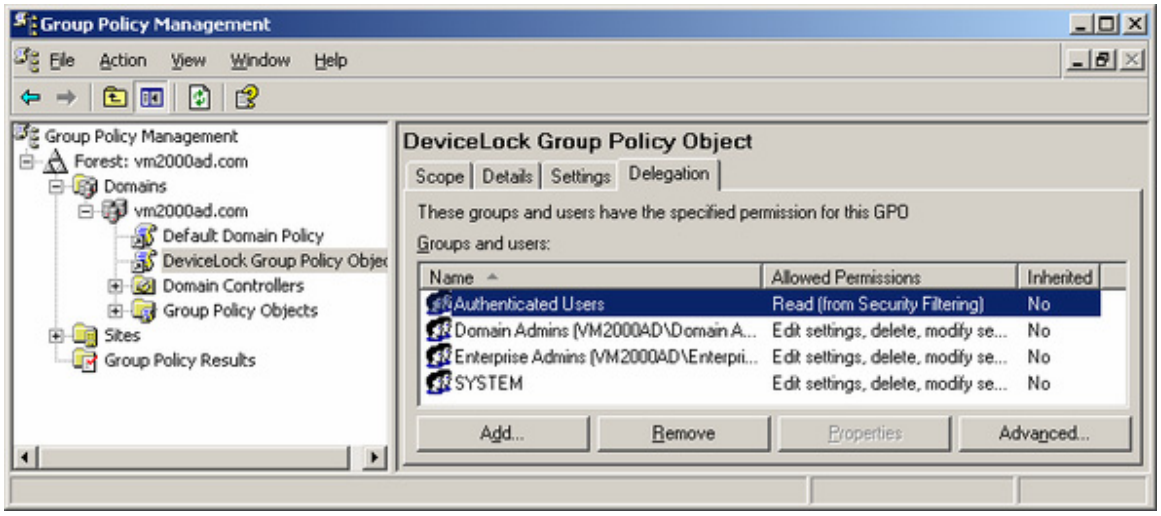
  3. Selezionare **Create and Link a GPO Here** dal menu contestuale.

     Se si sta utilizzando lo snap-in Utenti e computer di Active Directory, fare clic con il pulsante destro del mouse sul dominio, scegliere **Proprietà**, selezionare la scheda **Criteri di gruppo** e quindi scegliere **Nuovo**.

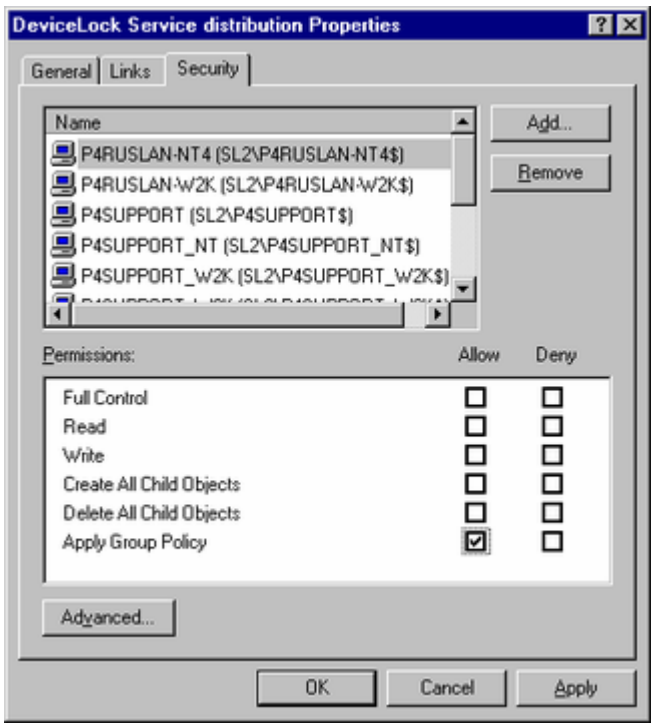




4. Digitare il nome da utilizzare per questi criteri e quindi premere **Invio**.
5. Nella struttura della console, selezionare l'oggetto Criteri di gruppo desiderato, scegliere la scheda **Delega** e quindi fare clic sul pulsante **Avanzate**.



Se si sta utilizzando lo snap-in Utenti e computer di Active Directory, scegliere **Proprietà** nella scheda **Criterio gruppo** e quindi selezionare la scheda **Protezione**.



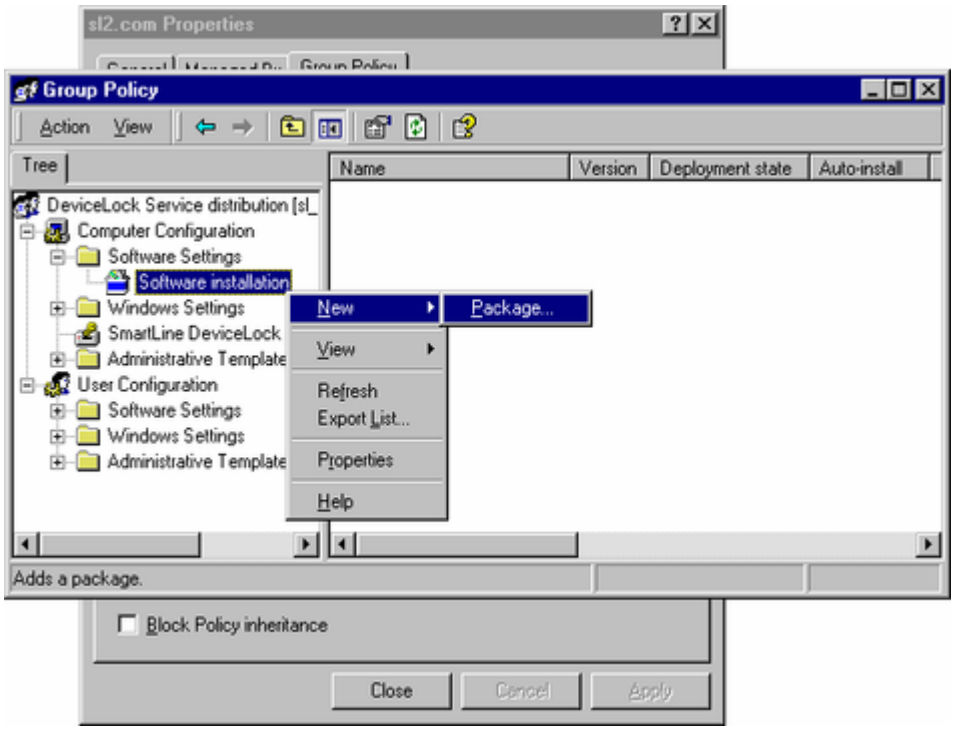
6. Selezionare la casella di controllo **Nega** a fianco della voce **Applica criteri di gruppo** per i gruppi di protezione a cui non si desidera applicare questo criterio.

   Selezionare la casella di controllo **Consenti** a fianco della voce **Applica criteri di gruppo** per i gruppi di protezione a cui si desidera applicare questo criterio. Una volta terminato, fare clic sul pulsante **OK**.

- **Assegnazione di un pacchetto**

  Per assegnare DeviceLock Service ai computer in cui è installato Windows 2000 o versione successiva:

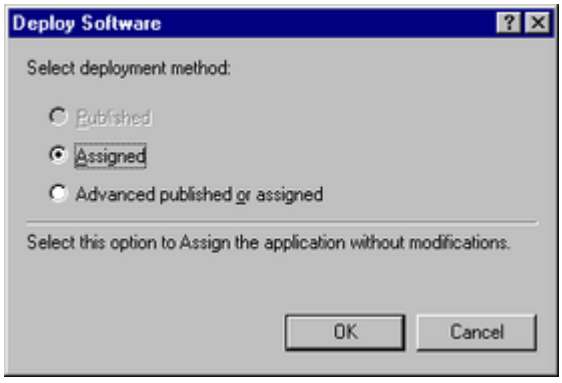
  1. Aprire lo snap-in Criterio gruppo e quindi selezionare l'oggetto Criteri di gruppo desiderato (è possibile utilizzare sia lo snap-in Gestione Criteri di gruppo, sia lo snap-in Utenti e computer di Active Directory).
  2. Espandere **Impostazioni del software** in corrispondenza di **Configurazione computer**.
  3. Fare clic con il pulsante destro del mouse su **Installazione software**, selezionare **Nuovo** e quindi **Package**.



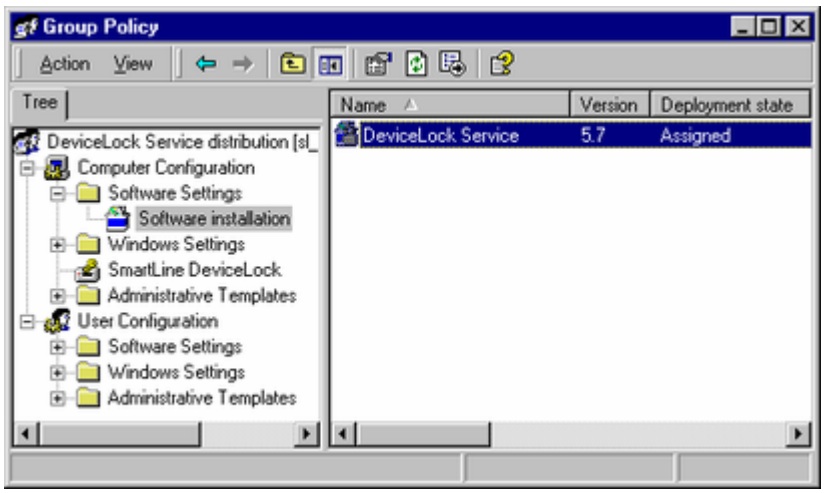
4. Nella finestra di dialogo **Apri**, digitare il percorso UNC (Universal Naming Convention) completo relativo alla cartella condivisa nella quale è memorizzato il pacchetto DeviceLock Service MSI. Ad esempio, \\file server\condivisione\DeviceLock Service.msi.

IMPORTANTE: non utilizzare il pulsante per individuare il percorso. Assicurarsi di specificare il percorso UNC per la cartella condivisa.

5. Fare clic sul pulsante **Apri**.
6. Scegliere l'opzione **Assegnato** e quindi fare clic sul pulsante **OK**. Il pacchetto verrà elencato nel riquadro destro della finestra **Criteri di gruppo**.



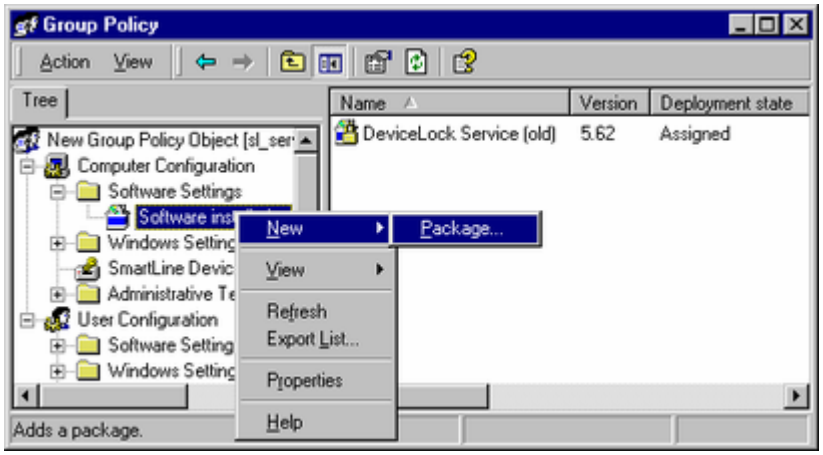
7. Chiudere lo snap-in Criterio gruppo. Quando il computer client viene avviato, verrà installato automaticamente DeviceLock Service.



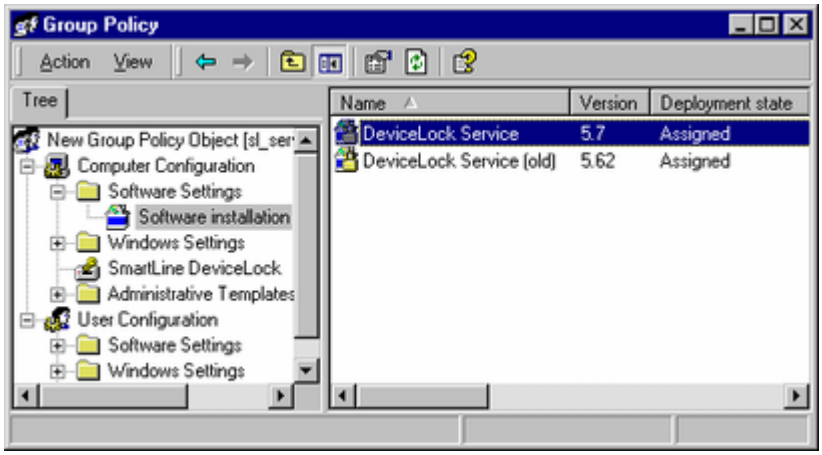
- **Aggiornamento di un pacchetto**

  Per ridistribuire DeviceLock Service se il pacchetto viene aggiornato:

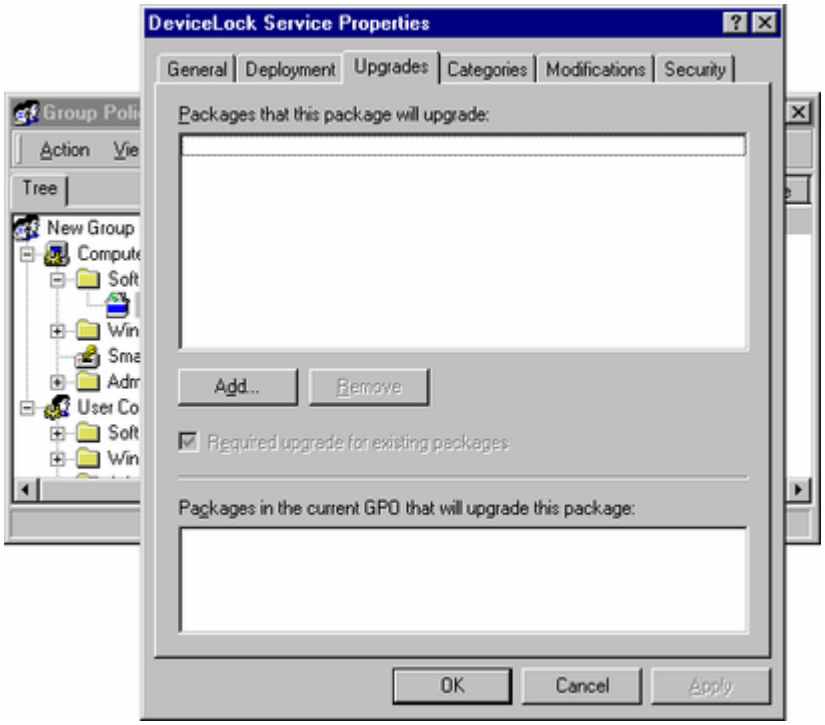
  1. Aprire lo snap-in Criterio gruppo e quindi selezionare l'oggetto Criteri di gruppo con cui è stato distribuito il vecchio pacchetto di DeviceLock Service (è possibile utilizzare sia lo snap-in Gestione Criteri di gruppo, sia lo snap-in Utenti e computer di Active Directory).
  2. Espandere **Impostazioni del software** in corrispondenza di **Configurazione computer**.
  3. Fare clic con il pulsante destro del mouse su **Installazione software**, selezionare **Nuovo** e quindi **Package**.



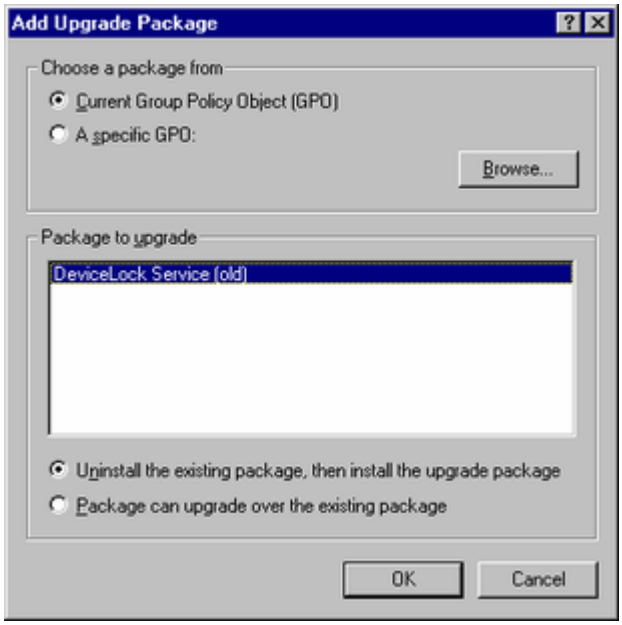
  4. Nella finestra di dialogo **Apri**, digitare il percorso UNC (Universal Naming Convention) completo relativo alla cartella condivisa nella quale è memorizzato il pacchetto DeviceLock Service MSI. Ad esempio, \\file server\condivisione\DeviceLock Service.msi.
  5. Fare clic sul pulsante **Apri**.
  6. Scegliere l'opzione **Assegnato** e quindi fare clic sul pulsante **OK**. Il pacchetto verrà elencato nel riquadro destro della finestra **Criteri di gruppo**.



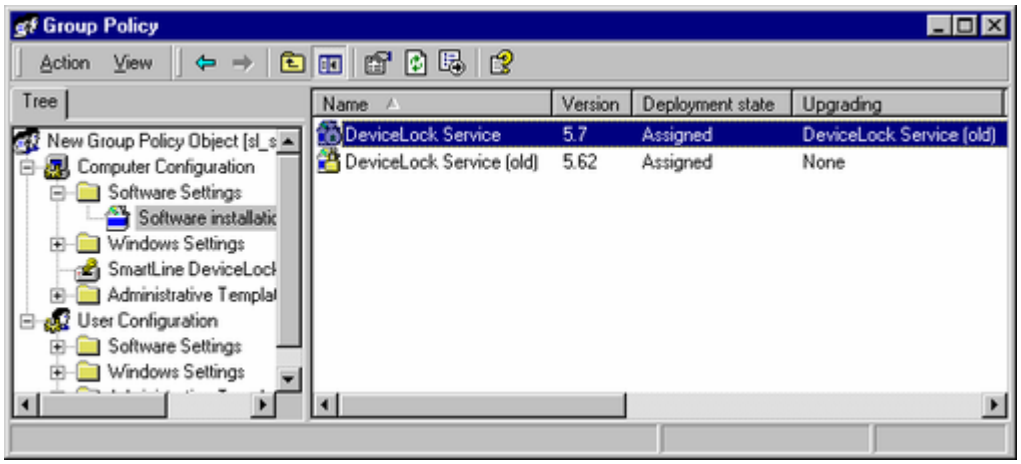
7. Fare clic on il pulsante destro del mouse sul nuovo pacchetto, scegliere **Proprietà** e quindi selezionare la scheda **Aggiornamenti**.



8. Fare clic sul pulsante **Aggiungi**, selezionare il vecchio pacchetto di DeviceLock Service che si desidera aggiornare, scegliere **Disinstalla il pacchetto esistente, quindi installa il pacchetto di aggiornamento** e quindi fare clic sul pulsante **OK**.



9. Scegliere **OK** per chiudere la finestra **Proprietà**, quindi chiudere lo snap-in Criterio gruppo. Quando il computer client viene avviato, verrà aggiornato automaticamente DeviceLock Service.



Nota: generalmente, quando si aggiorna, il nuovo pacchetto MSI di DeviceLock Service rileva il pacchetto precedentemente assegnato all'oggetto Criteri di gruppo ed esegue automaticamente i passaggi 7 e 8 descritti sopra.

- **Ridistribuzione di un pacchetto**

  In alcuni casi può essere necessario ridistribuire DeviceLock Service.

  Per ridistribuire un pacchetto:

  1. Aprire lo snap-in Criterio gruppo e quindi selezionare l'oggetto Criteri di gruppo con cui è stato distribuito il pacchetto di DeviceLock Service (è possibile utilizzare sia lo snap-in Gestione Criteri di gruppo, sia lo snap-in Utenti e computer di Active Directory).

2. Espandere il contenitore **Impostazioni del software** che include l'elemento **Installazione software** con cui è stato distribuito il pacchetto.
3. Fare clic sul contenitore **Installazione software** che include il pacchetto.
4. Nel riquadro destro della finestra **Criterio gruppo** fare clic con il pulsante destro del mouse sul programma, scegliere **Tutte le attività** e quindi **Ridistribuisci applicazione**. Verrà visualizzato il seguente messaggio (o messaggio analogo): "La ridistribuzione di questa applicazione ne determina la reinstallazione ovunque sia già installata. Continuare?".
5. Fare clic su **Sì**.
6. Chiudere lo snap-in Criterio gruppo.

- **Rimozione di un pacchetto**

  Per rimuovere DeviceLock Service:

  1. Aprire lo snap-in Criterio gruppo e quindi selezionare l'oggetto Criteri di gruppo con cui è stato distribuito DeviceLock Service (è possibile utilizzare sia lo snap-in Gestione Criteri di gruppo, sia lo snap-in Utenti e computer di Active Directory).
  2. Espandere il contenitore **Impostazioni del software** che include l'elemento **Installazione software** con cui è stato distribuito il pacchetto.
  3. Fare clic sul contenitore **Installazione software** che include il pacchetto.
  4. Nel riquadro destro della finestra **Criterio gruppo** fare clic con il pulsante destro del mouse sul programma, scegliere **Tutte le attività** e quindi **Rimuovi**.
  5. Fare clic su **Disinstalla immediatamente il software per utenti e computer** e quindi scegliere **OK**.
  6. Chiudere lo snap-in Criterio gruppo.

Si consiglia di tenere presente quanto segue:

- La distribuzione viene eseguita solamente durante l'avvio del computer e non su base periodica. Questo consente di prevenire risultati indesiderati, quali la disinstallazione o l'aggiornamento di un'applicazione in uso.
- DeviceLock Service viene copiato nella cartella %ProgramFiles%\DeviceLock Agent, se questo servizio non è presente sul sistema in uso. Se il servizio è presente sul sistema in uso ma la versione è inferiore a 7.0, DeviceLock Service viene copiato anche nella cartella predefinita %ProgramFiles%\DeviceLock Agent. Se il servizio è presente sul sistema in uso ma la versione è uguale o superiore a 7.0, DeviceLock Service viene copiato nella directory già presente, sostituendo i file precedenti.

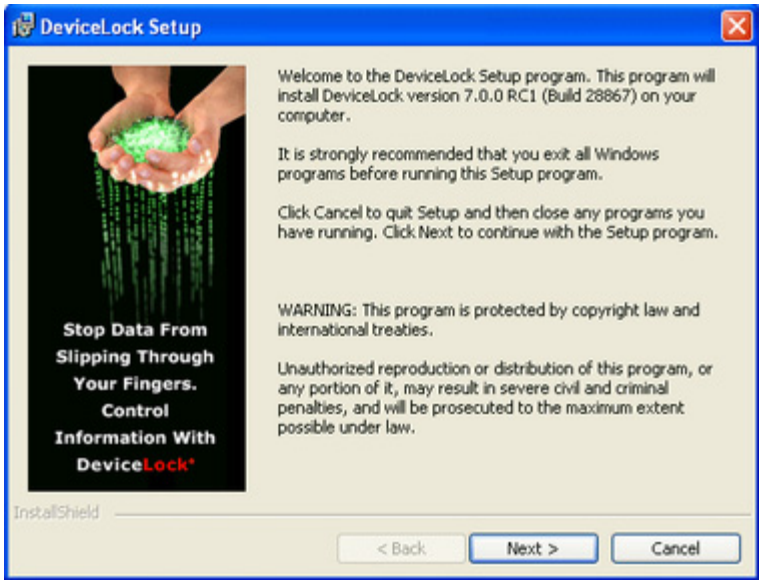
Installazione delle console di gestione

Le console di gestione sono interfacce di controllo che consentono agli amministratori di sistema di gestire in remoto DeviceLock Service, DeviceLock Enterprise Server e DeviceLock Content Security Server.

Le console di gestione dovrebbero essere installate sui computer che gli amministratori di sistema intendono utilizzare per gestire le impostazioni di DeviceLock e per avviare i report. Non è necessario installare le console di gestione sul server (controller di dominio o altro), anche qualora si intenda utilizzare il gestore dei criteri di gruppo di DeviceLock per gestire le impostazioni tramite i Criteri di gruppo di Active Directory - è sufficiente utilizzare la propria workstation (naturalmente, è necessario disporre dei privilegi necessari).

Nota: per utilizzare DeviceLock Management Console (lo snap-in MMC) e DeviceLock Service Settings Editor su un computer che esegue Windows NT 4.0, è necessario aggiornare Microsoft Management Console. È possibile scaricare gratuitamente questo aggiornamento dal sito Web di Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=3F620A07-C996-4A81-AAD8-30134A43EC46&displaylang=en.

Avviare il programma di installazione (**setup.exe**) e seguire le istruzioni che compaiono sullo schermo.

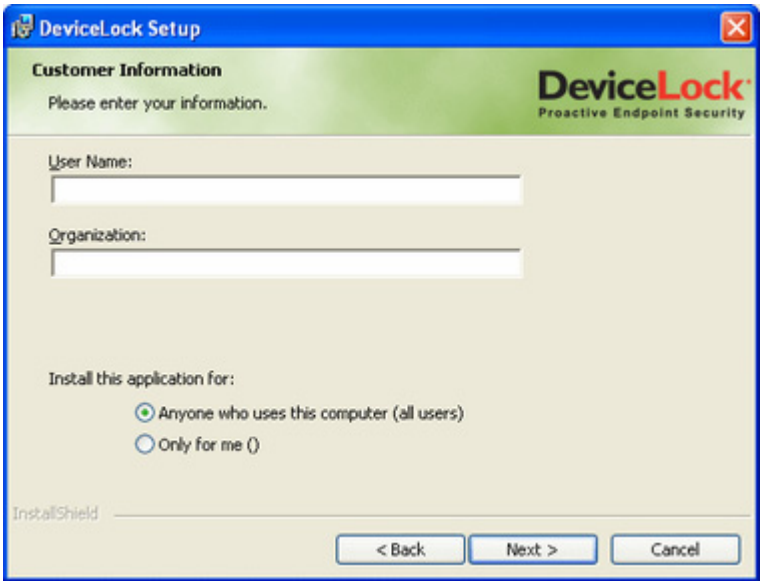

DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

Per proseguire con l'installazione, è necessario accettare le clausole del Contratto di licenza con l'utente finale.

Nella pagina **Customer Information**, digitare il proprio nome utente e il nome dell'organizzazione. Nella stessa pagina, nella sezione **Install this application for** è possibile specificare i collegamenti sul desktop da creare per le console di gestione di DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager e

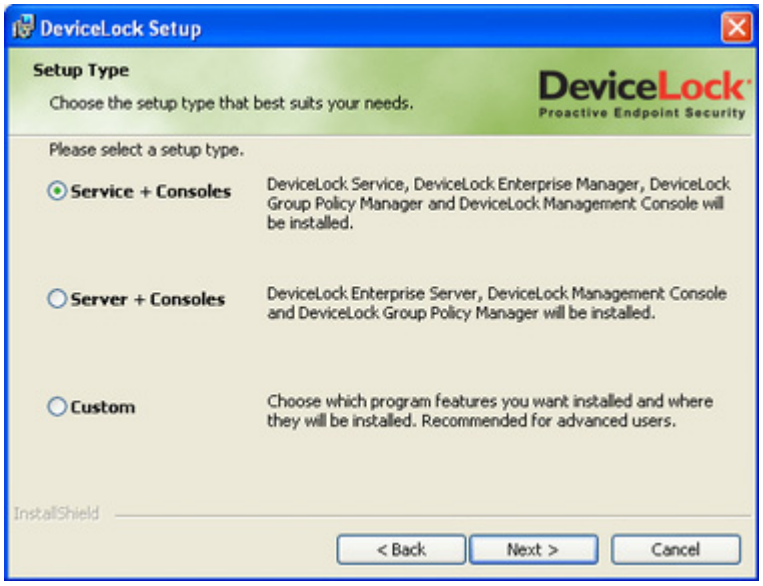
DeviceLock Service Settings Editor). È possibile selezionare una delle seguenti opzioni:

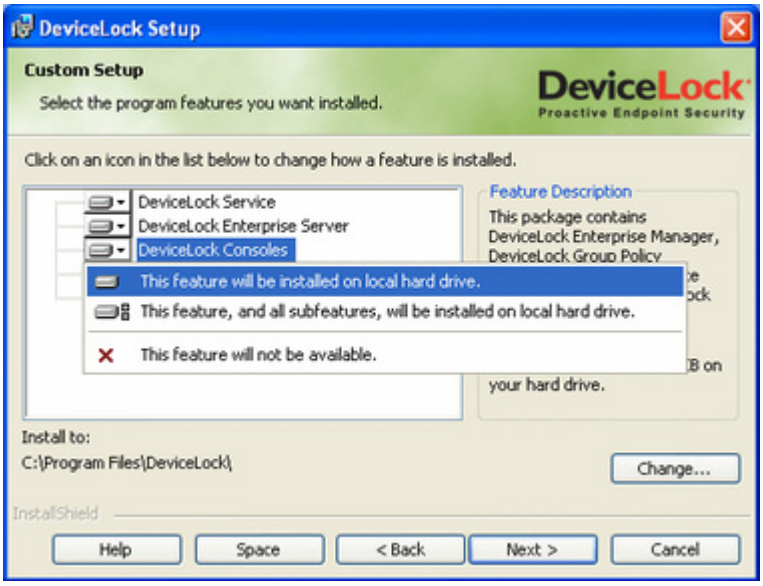
- **Anyone who uses this computer (all users)**: crea collegamenti sul desktop sulle console di gestione di DeviceLock per tutti gli utenti.
- **Only for me**: crea collegamenti sul desktop sulle console di gestione di DeviceLock solo per l'account che sta installando DeviceLock.



Nella pagina **Setup type**, selezionare il tipo di installazione desiderata.

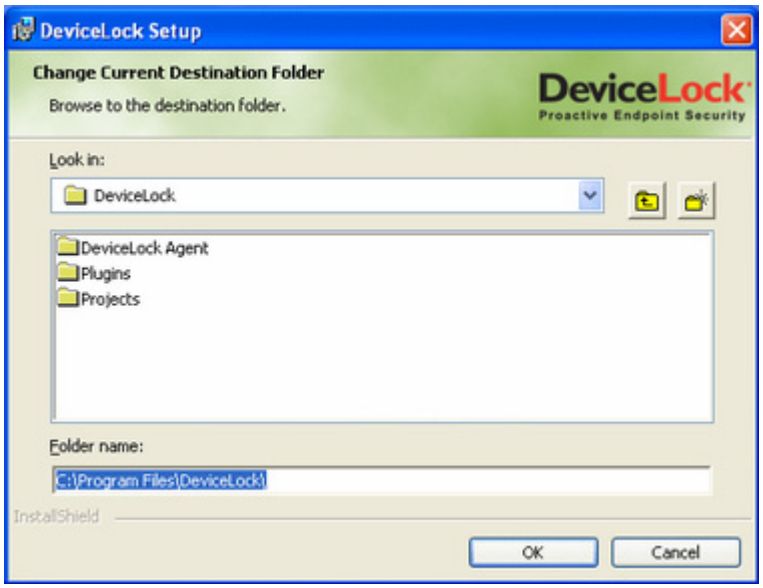
È possibile effettuare una delle tre seguenti scelte: installare DeviceLock Service e le console di gestione di DeviceLock selezionando l'opzione **Service + Consoles**, installare DeviceLock Enterprise Server e le console gestione di DeviceLock selezionando l'opzione **Server + Consoles** oppure installare solamente le console di gestione di DeviceLock scegliendo l'opzione **Custom** e quindi selezionando il componente **DeviceLock Consoles**.


DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel


DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
DeviceLock Enterprise Server
DeviceLock Consoles
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
Feature Description
This package contains DeviceLock Enterprise Manager, DeviceLock Group Policy
your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

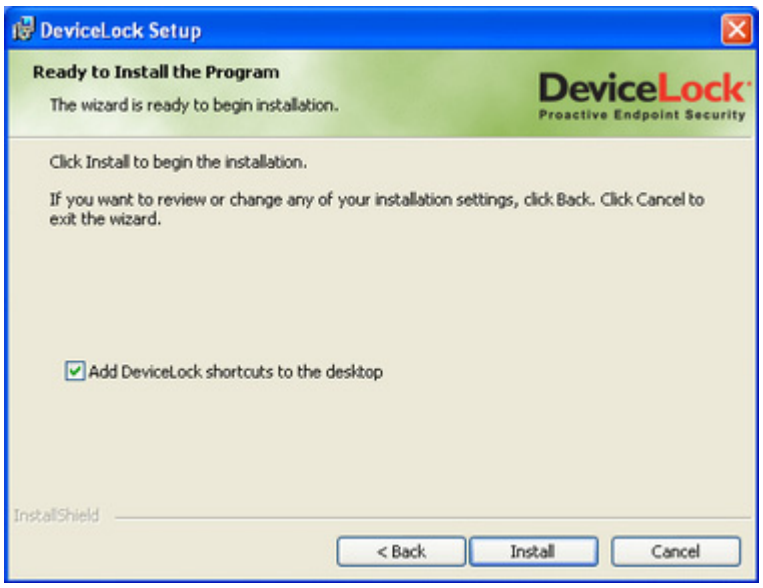
Nota: nella pagina **Custom Setup** è possibile selezionare il componente RSoP (Resultant Set of Policy: Gruppo di criteri risultante) da installare. Quest'ultimo attiva il supporto della modalità di pianificazione RSoP di DeviceLock sui controller di dominio. Il componente RSoP è richiesto unicamente quando sul computer in uso sono installate le console di gestione DeviceLock, mentre DeviceLock Service non è installato. Per ulteriori informazioni sulla modalità di pianificazione RSoP, consultare la documentazione di Microsoft.

Nella pagina **Custom Setup** è possibile modificare le directory di installazione predefinita. La directory di installazione predefinita di DeviceLock è **%ProgramFiles%\DeviceLock**. Per modificare la directory di installazione predefinita, fare clic su **Change** per aprire la pagina **Change Current Destination Folder**.



DeviceLock viene distribuito con tre console di gestione differenti: DeviceLock Management Console (lo snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Group Policy Manager (integrato nell'Editor oggetti Criteri di gruppo). DeviceLock Service Settings Editor, installato unitamente alle altre console di gestione, è uno strumento utilizzato per creare e modificare file XML esterni introducendo impostazioni, autorizzazioni, regole di controllo e di shadowing per DeviceLock Service.

Nella pagina **Ready to Install the Program**, fare clic su **Install** per avviare l'installazione. Selezionare la casella di controllo **Add DeviceLock shortcuts to the desktop** per aggiungere i collegamenti a DeviceLock Management Console (lo snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Service Settings Editor sul desktop.

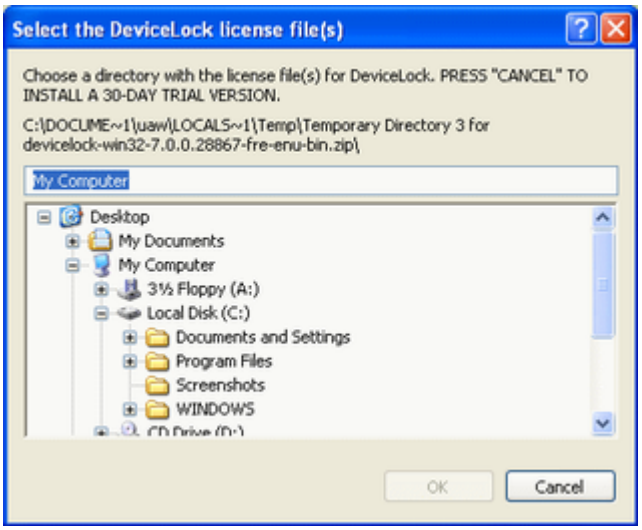

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Il programma di installazione chiederà di creare un nuovo certificato di DeviceLock.

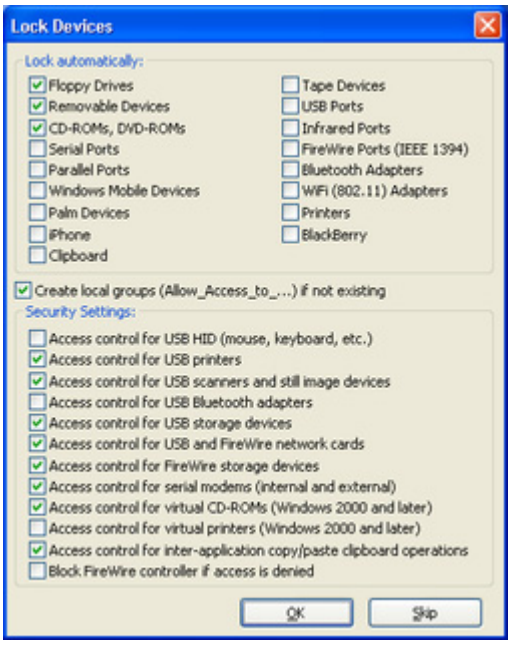
DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

È possibile creare un nuovo certificato di DeviceLock anche successivamente, utilizzando lo strumento di generazione dei certificati installato assieme alle console di gestione di DeviceLock. Quindi, in caso di dubbio, fare clic sul pulsante **No** e proseguire con l'installazione. Per ulteriori informazioni sui certificati di DeviceLock, consultare la sezione "Certificati di DeviceLock".

Inoltre, potrebbe essere visualizzato un messaggio in cui si richiede il caricamento dei file di licenza di DeviceLock. Qualora non si sia in possesso del file della licenza, fare clic sul pulsante **Cancel**: DeviceLock verrà installato in modalità di valutazione e sarà valido per 30 giorni.

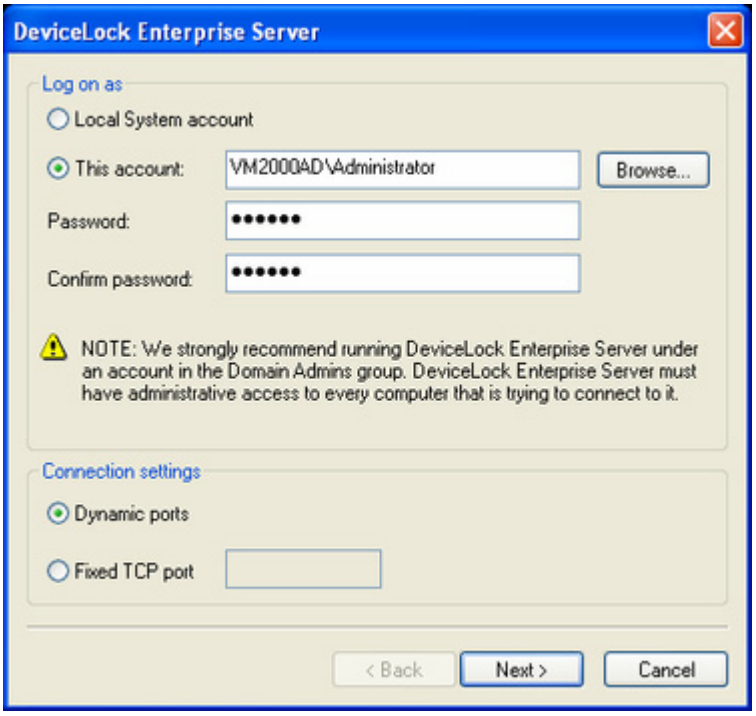


Se si è scelto di installare anche DeviceLock Service, il programma di installazione consiglierà di applicare speciali autorizzazioni alle periferiche locali.



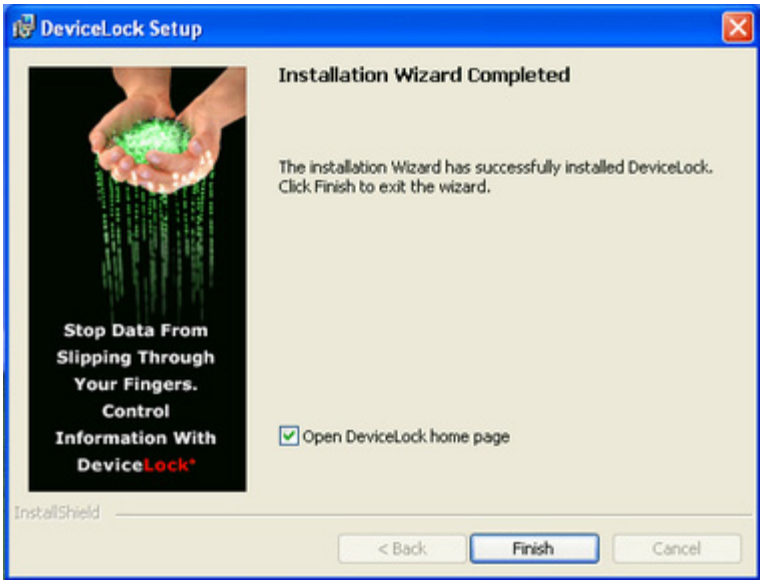
Se si preferisce assegnare le autorizzazioni tramite le console di gestione di DeviceLock al termine dell'installazione del software, fare clic sul pulsante **Skip**. Per ulteriori informazioni sulle autorizzazioni, leggere la sezione Distribuzione di DeviceLock Service.

Se si è scelto di installare anche DeviceLock Enterprise Server, il programma di installazione consentirà di configurarne le impostazioni tramite una procedura guidata.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

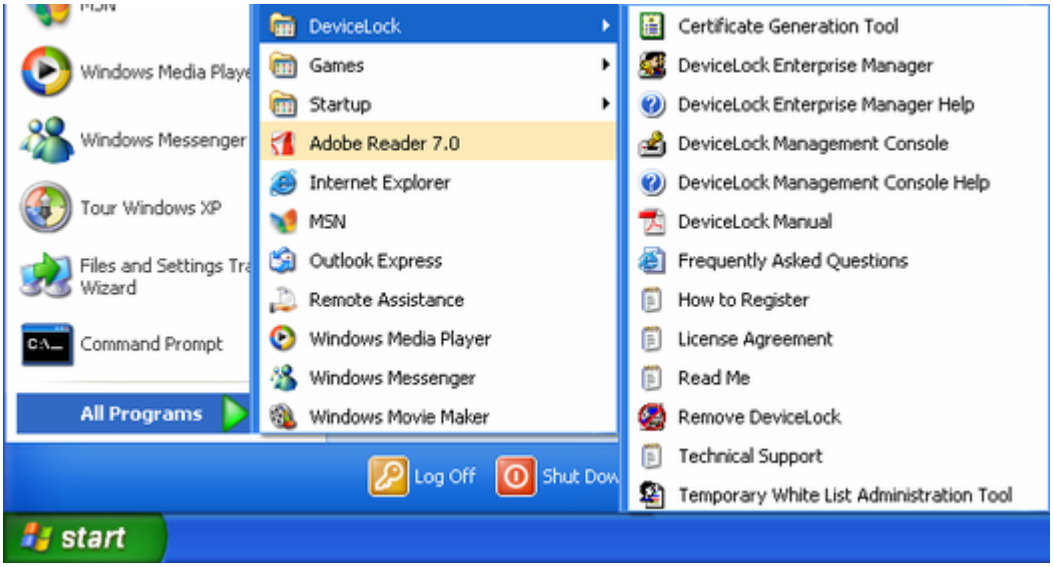
Per ulteriori informazioni sulle impostazioni di DeviceLock Enterprise Server, leggere la sezione Installazione di DeviceLock Enterprise Server.

Una volta completata l'installazione del software, il programma di installazione consiglierà di visitare il sito Web di DeviceLock.


DeviceLock Setup
Installation Wizard Completed
The installation Wizard has successfully installed DeviceLock. Click Finish to exit the wizard.
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Open DeviceLock home page
InstallShield
< Back
Finish
Cancel

Deselezionare la casella di controllo **Open DeviceLock home page** se non si desidera visitare il sito Web di DeviceLock. Fare clic su **Finish** per terminare l'installazione.

Per avviare le console di gestione di DeviceLock, fare clic sul pulsante **Start** e scegliere **Tutti i programmi**.



Nota: DeviceLock Group Policy Manager si integra nello snap-in Criterio gruppo e non è disponibile come applicazione a sé stante. Per avviare DeviceLock Group Policy Manager, è necessario eseguire lo snap-in Criterio gruppo.

Per disinstallare DeviceLock, eseguire una delle seguenti azioni:

Aprire **Installazione applicazioni** nel Pannello di controllo per rimuovere **DeviceLock**.
- OPPURE -
Fare clic su **Start**, selezionare **Tutti i programmi**, **DeviceLock**, quindi fare clic su **Remove DeviceLock**.

Installazione di DeviceLock Enterprise Server

DeviceLock Enterprise Server è un componente opzionale che consente di centralizzare la raccolta e l'archiviazione delle copie shadow dei dati e dei registri degli eventi. Inoltre, DeviceLock Enterprise Server è in grado di monitorare i computer remoti in tempo reale, verificando lo stato di DeviceLock Service (attivo o meno) e l'uniformità e l'integrità dei criteri.

Per utilizzare DeviceLock Enterprise Server su un computer che esegue Windows NT 4.0 SP6 e Windows 2000, è necessario installare Microsoft Data Access Components (MDAC) 2.8 o versione successiva. È possibile scaricare gratuitamente MDAC dal sito Web di Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&displaylang=it.

Progettazione dell'infrastruttura

Per bilanciare meglio il carico della rete, è possibile installare DeviceLock Enterprise Server su più computer differenti.

DeviceLock Enterprise Server utilizza Microsoft SQL Server per archiviare i propri dati. Prima di installare DeviceLock Enterprise Server, è quindi necessario che sia installato ed in esecuzione Microsoft SQL Server. Se non si dispone di Microsoft SQL Server, è possibile scaricare gratuitamente l'edizione Express di Microsoft SQL Server dal sito Web di Microsoft:
http://www.microsoft.com/sqlserver/2005/en/us/express.aspx.

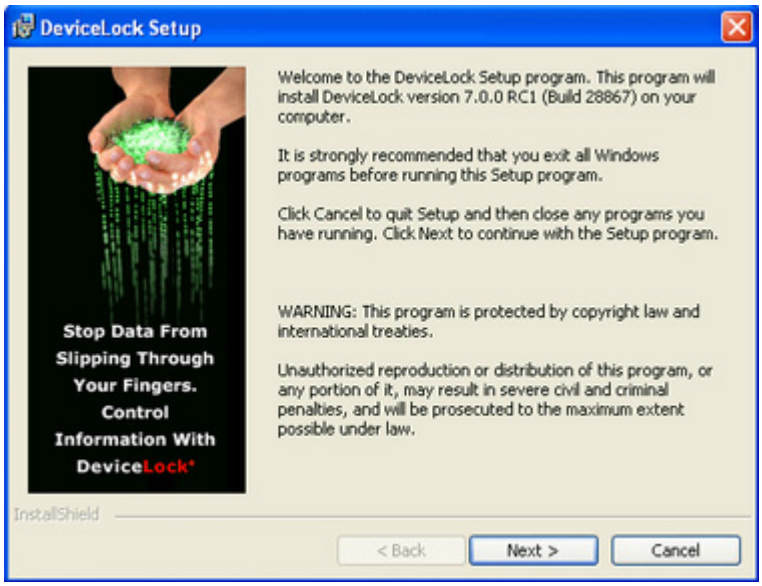
Non è necessario eseguire Microsoft SQL Server e DeviceLock Enterprise Server sulla stessa macchina. Per garantire stabilità e prestazioni, è preferibile infatti installare il componente DeviceLock Enterprise Server su un computer separato.

Sono disponibili tre scenari aziendali che descrivono altrettante soluzioni di connessione tra DeviceLock Enterprise Server e Microsoft SQL Server. Prima di installare DeviceLock Enterprise Server, è preferibile scegliere lo scenario che meglio si adatta alle proprie esigenze:

1. UNO-A-UNO: DeviceLock Enterprise Server viene installato su una singola macchina e viene connesso ad una singola istanza di Microsoft SQL Server. Questo scenario è il più adatto per reti di piccole dimensioni (fino a diverse centinaia di computer).
2. MOLTI-A-MOLTI: DeviceLock Enterprise Server viene installato su più macchine e ciascuno di essi viene connesso ad un propria istanza di Microsoft SQL Server. Questo è il tipico scenario per reti di medie e grandi dimensioni geograficamente distribuite in diversi segmenti.
3. MOLTI-A-UNO: DeviceLock Enterprise Server viene installato su più macchine e tutti vengono connessi ad un'unica istanza di Microsoft SQL Server. Questo scenario potrebbe essere il più adatto per reti di medie e grandi dimensioni dotate di una macchina potente dedicata a Microsoft SQL Server (ovvero un computer dotato di una grande quantità di memoria e in cui sia disponibile una grande quantità di spazio di archiviazione).

Installazione interattiva

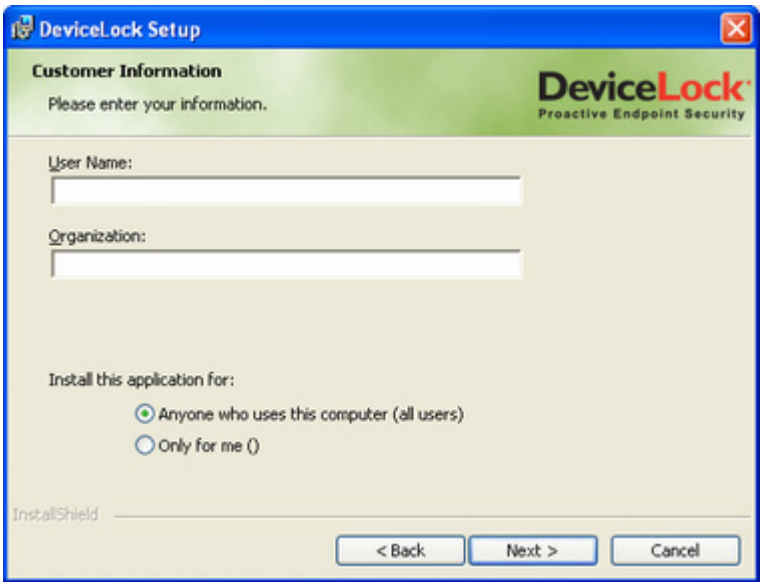
Avviare il programma di installazione (**setup.exe**) e seguire le istruzioni che compaiono sullo schermo. Eseguire il programma **setup.exe** su ciascun computer su cui sarà installato DeviceLock Enterprise Server.


DeviceLock Setup
Stop Data From Slipping Through Your Fingers. Control Information With DeviceLock
Welcome to the DeviceLock Setup program. This program will install DeviceLock version 7.0.0 RC1 (Build 28867) on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
< Back
Next >
Cancel

Per proseguire con l'installazione, è necessario accettare le clausole del Contratto di licenza con l'utente finale.

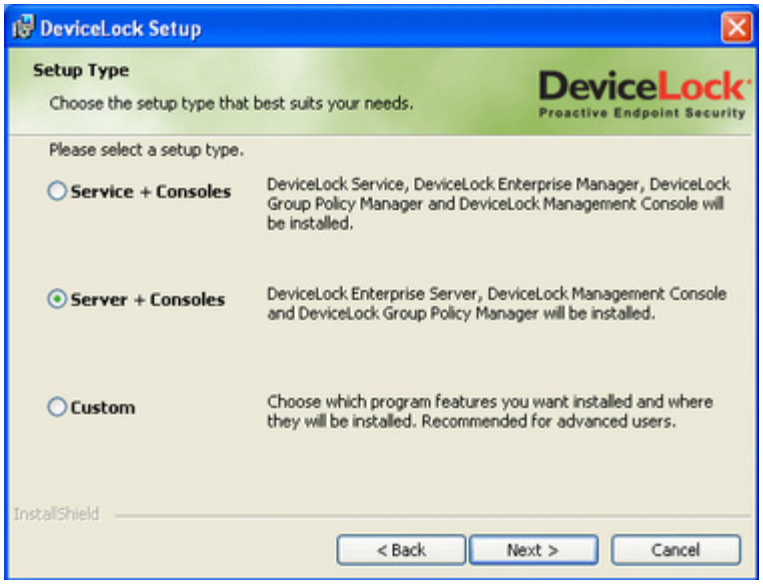
Nella pagina **Customer Information**, digitare il proprio nome utente e il nome dell'organizzazione. Nella stessa pagina, nella sezione **Install this application for** è possibile specificare i collegamenti sul desktop da creare per le console di gestione di DeviceLock (DeviceLock Management Console, DeviceLock Enterprise Manager e DeviceLock Service Settings Editor). È possibile selezionare una delle seguenti opzioni:

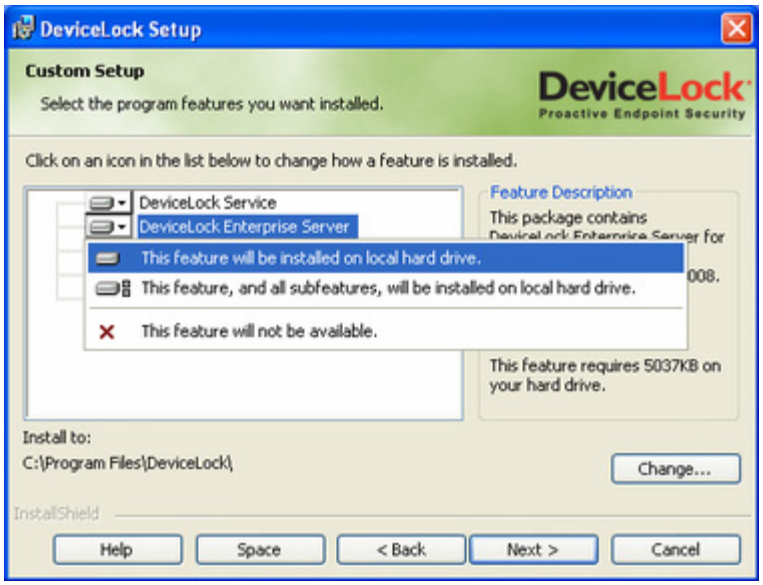
- **Anyone who uses this computer (all users)**: crea collegamenti sul desktop sulle console di gestione di DeviceLock per tutti gli utenti.
- **Only for me**: crea collegamenti sul desktop sulle console di gestione di DeviceLock solo per l'account che sta installando DeviceLock.



Nella pagina **Setup type**, selezionare il tipo di installazione desiderata.

È possibile effettuare una delle due seguenti scelte: installare DeviceLock Enterprise Server e le console di gestione di DeviceLock selezionando l'opzione **Server + Consoles** oppure installare solamente DeviceLock Enterprise Server selezionando l'opzione **Custom** e quindi selezionando il componente **DeviceLock Enterprise Server**.

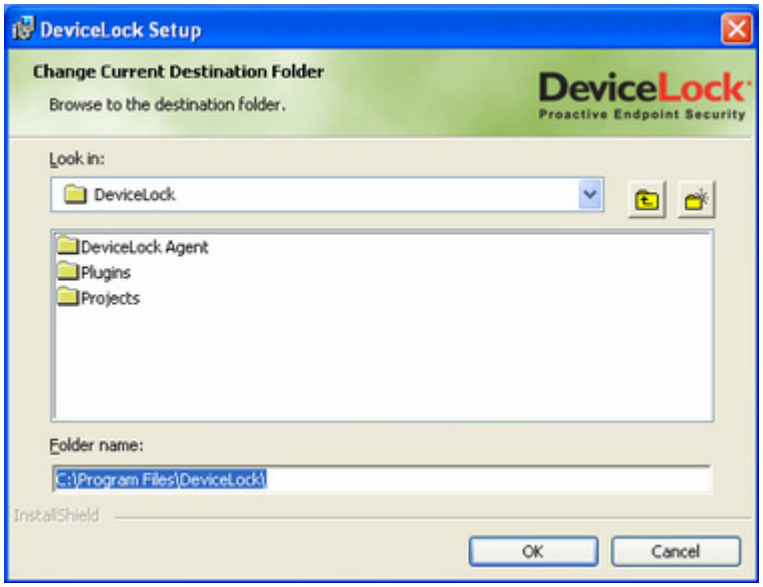

DeviceLock Setup
Setup Type
Choose the setup type that best suits your needs.
DeviceLock
Proactive Endpoint Security
Please select a setup type.
Service + Consoles
DeviceLock Service, DeviceLock Enterprise Manager, DeviceLock Group Policy Manager and DeviceLock Management Console will be installed.
Server + Consoles
DeviceLock Enterprise Server, DeviceLock Management Console and DeviceLock Group Policy Manager will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel


DeviceLock Setup
Custom Setup
Select the program features you want installed.
DeviceLock
Proactive Endpoint Security
Click on an icon in the list below to change how a feature is installed.
DeviceLock Service
DeviceLock Enterprise Server
Feature Description
This package contains
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.
This feature requires 5037KB on your hard drive.
Install to:
C:\Program Files\DeviceLock\
Change...
InstallShield
Help
Space
< Back
Next >
Cancel

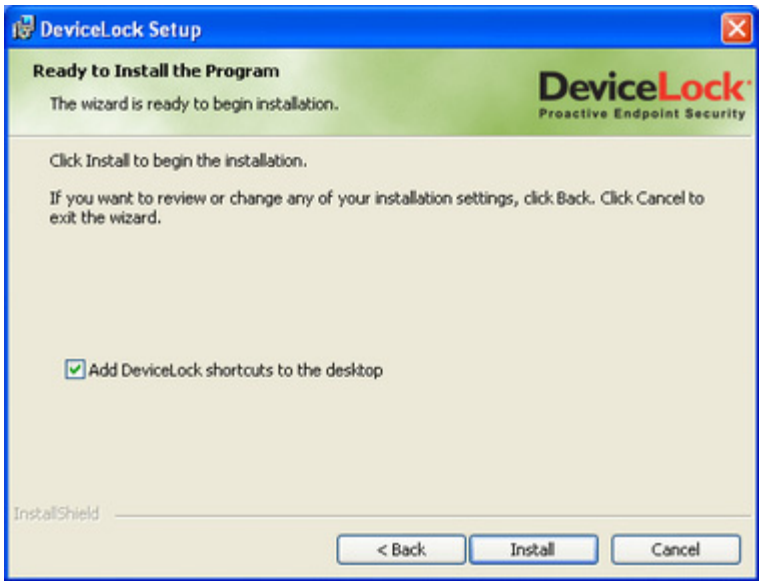
Nota: nella pagina **Custom Setup** è possibile selezionare il componente RSoP (Resultant Set of Policy: Gruppo di criteri risultante) da installare. Quest'ultimo attiva il supporto della modalità di pianificazione RSoP di DeviceLock sui controller di dominio. Il componente RSoP è

richiesto unicamente quando sul computer in uso sono installate le console di gestione DeviceLock, mentre DeviceLock Service non è installato. Per ulteriori informazioni sulla modalità di pianificazione RSoP, consultare la documentazione di Microsoft.

Nella pagina **Custom Setup** è possibile modificare le directory di installazione predefinita. La directory di installazione predefinita di DeviceLock è **%ProgramFiles%\DeviceLock**. Per modificare la directory di installazione predefinita, fare clic su **Change** per aprire la pagina **Change Current Destination Folder**.



Nella pagina **Ready to Install the Program**, fare clic su **Install** per avviare l'installazione. Selezionare la casella di controllo **Add DeviceLock shortcuts to the desktop** per aggiungere i collegamenti a DeviceLock Management Console (lo snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Service Settings Editor sul desktop.

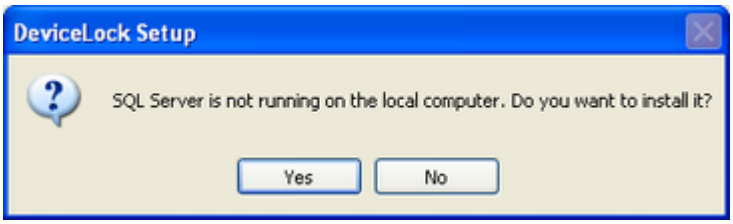

DeviceLock Setup
Ready to Install the Program
The wizard is ready to begin installation.
DeviceLock
Proactive Endpoint Security
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Add DeviceLock shortcuts to the desktop
InstallShield
< Back
Install
Cancel

Qualora si sia scelto di installare le console di gestione di DeviceLock, il programma di installazione chiederà di creare un nuovo certificato di DeviceLock.

DeviceLock Setup
Do you want to create the new DeviceLock Certificate (the private and public key pair)?
Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair.
Yes
No

È possibile creare un nuovo certificato di DeviceLock anche successivamente, utilizzando lo strumento di generazione dei certificati installato assieme alle console di gestione di DeviceLock. Quindi, in caso di dubbio, fare clic sul pulsante **No** e proseguire con l'installazione. Per ulteriori informazioni sui certificati di DeviceLock, consultare la sezione "Certificati di DeviceLock".

Se il programma di installazione rileva che Microsoft SQL Server non è in esecuzione sul computer locale, chiederà di installarlo qualora sia disponibile il relativo pacchetto di distribuzione.



Se non si desidera installare Microsoft SQL Server sul computer locale oppure Microsoft SQL Server è già installato ma non è stato avviato, fare clic sul pulsante **No**.

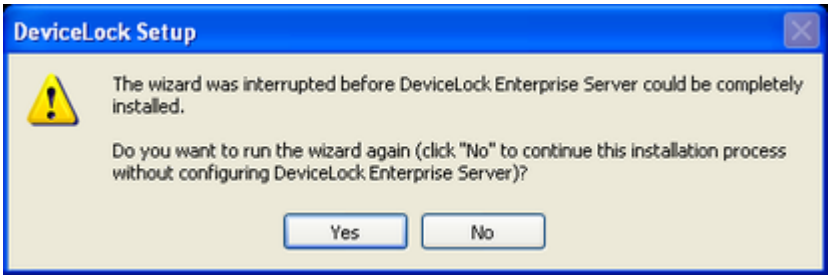
Durante la fase di installazione, una speciale procedura guidata consentirà di configurare le impostazioni principali di DeviceLock Enterprise Server.

Se si sta provvedendo ad un aggiornamento o ad una reinstallazione di DeviceLock Enterprise Server e si desidera mantenere la configurazione corrente del programma, fare clic sul pulsante **Annulla** per chiudere la procedura guidata senza modificare le opzioni del software.

Per modificare invece solo alcuni dei parametri di configurazione di DeviceLock Enterprise Server, proseguire con la procedura guidata e modificare solamente le impostazioni necessarie, fino a quando non si rende disponibile il pulsante **Fine** sull'ultima pagina.

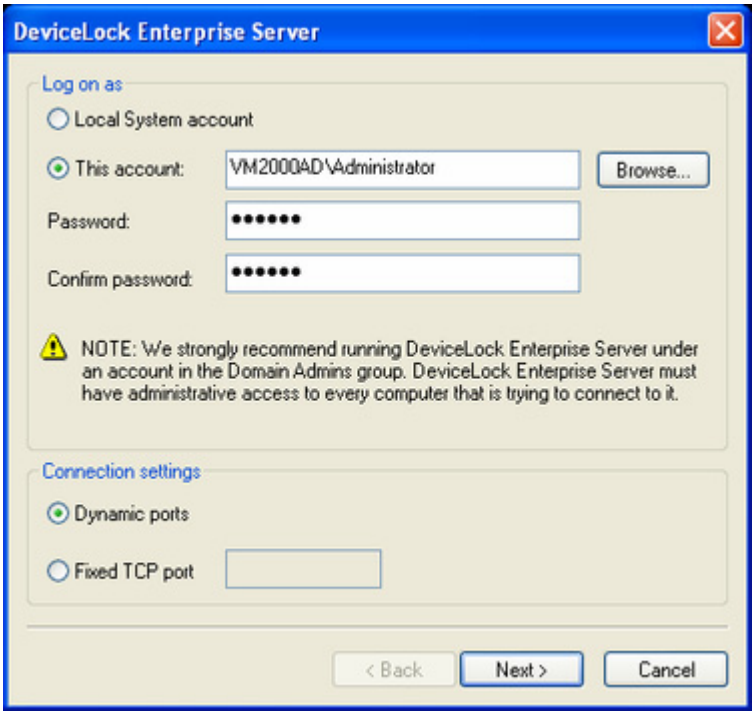
Nota: se si installa DeviceLock Enterprise Server per la prima volta su un computer e si interrompe la procedura di configurazione guidata, il programma di installazione non sarà in grado di installare il servizio di DeviceLock Enterprise Server. Per completare l'installazione del

servizio di DeviceLock Enterprise Server sarà quindi necessario avviare nuovamente la procedura di configurazione guidata.


DeviceLock Setup
The wizard was interrupted before DeviceLock Enterprise Server could be completely installed.
Do you want to run the wizard again (click "No" to continue this installation process without configuring DeviceLock Enterprise Server)?
Yes
No

Se si fa clic sul pulsante **No** per proseguire l'installazione senza installare il servizio di DeviceLock Enterprise Server, successivamente sarà necessario avviare nuovamente il programma di installazione per installare il servizio.

La prima pagina della procedura guidata consente di installare il servizio di DeviceLock Enterprise Server e di configurare i parametri di avvio.


DeviceLock Enterprise Server
Log on as
Local System account
This account:
VM2000AD\Administrator
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.
Connection settings
Dynamic ports
Fixed TCP port
< Back
Next >
Cancel

Gruppo di opzioni "Log on as"
Innanzitutto, scegliere con quale account avviare il servizio di DeviceLock Enterprise Server. Così come per molti altri servizi di Windows, è possibile avviare il servizio di DeviceLock Enterprise Server con l'account di sistema locale (utente SYSTEM) o con qualsiasi altro account utente.

Per avviare il servizio con l'account utente SYSTEM, selezionare l'opzione **Local System account**. È bene ricordare che i processi eseguiti dall'account utente

SYSTEM non possono accedere alle risorse di rete condivise e non possono autenticarsi sui computer remoti con credenziali anonime. I componenti DeviceLock Enterprise Server configurati per essere avviati con l'account utente SYSTEM non sono quindi in grado di archiviare le copie shadow dei dati sui computer remoti (ad esempio, su un file server) e pertanto, per autenticarsi, devono utilizzare i certificati di DeviceLock.

Per ulteriori informazioni sui metodi di autenticazione, leggere la descrizione del parametro Certificate Name.

Per avviare il servizio con le credenziali di un utente, selezionare l'opzione **This account**, quindi immettere il nome account dell'utente e la password. Si consiglia di utilizzare un account utente che disponga dei privilegi amministrativi su tutti i computer sui quali DeviceLock Service è in esecuzione. In caso contrario, per effettuare l'autenticazione, sarà necessario utilizzare il certificato di DeviceLock.

Se si sta installando DeviceLock Enterprise Server in un ambiente di dominio, si consiglia di utilizzare un account utente che sia membro del gruppo Domain Admins. Poiché il gruppo Domain Admins è membro del gruppo locale Administrators su ciascun computer appartenente al dominio, i membri del gruppo Domain Admins avranno accesso completo a DeviceLock Service su ogni computer.

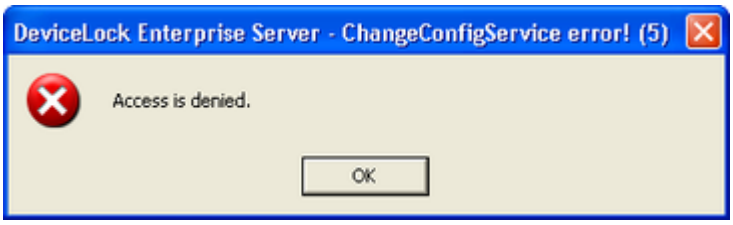
È bene ricordare che, se DeviceLock Security è attivo sui computer remoti che eseguono DeviceLock Service per proteggere questi ultimi da accessi non autorizzati da parte di utenti locali che dispongono di privilegi amministrativi, l'account utente specificato nell'opzione **This account** deve essere incluso anche nell'elenco degli amministratori di DeviceLock e deve disporre del privilegio **Full access**. In caso contrario, per effettuare l'autenticazione, sarà necessario utilizzare il certificato di DeviceLock.

Gruppo di opzioni "Connection settings"
DeviceLock Enterprise Server può utilizzare una porta TCP fissa per comunicare con la console di gestione. Questo consente di configurare più facilmente un firewall. Immettere il numero della porta desiderato nel campo **Fixed TCP port**. Per utilizzare le porte dinamiche RPC, selezionare l'opzione **Dynamic ports**. Per impostazione predefinita, DeviceLock Enterprise Server utilizza la porta 9133.

Fare clic sul pulsante **Avanti** per avviare il servizio di DeviceLock Enterprise Server e proseguire alla seconda pagina della procedura guidata.

Se si sta installando un aggiornamento di DeviceLock Enterprise Server ma l'utente corrente non dispone di privilegi amministrativi completi per accedere a DeviceLock Enterprise Server, la procedura di configurazione guidata non sarà in grado di installare il servizio e di applicare le modifiche. Inoltre, se si sta effettuando l'installazione di DeviceLock Enterprise Server su un computer su cui l'utente

corrente non dispone di privilegi amministrativi locali, sarà visualizzato un messaggio di errore simile al seguente:



Se si seleziona l'opzione **This account** e si specifica un nome utente o una password non validi, non sarà possibile avviare DeviceLock Enterprise Server.

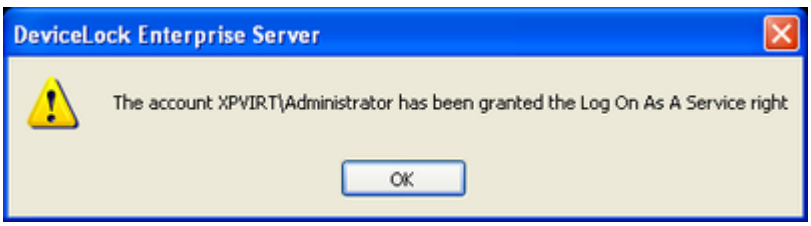
DeviceLock Enterprise Server - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

Se si seleziona l'opzione **This account** e si specifica un account utente che non è membro del gruppo Domain Admins, sarà visualizzato un messaggio di notifica.

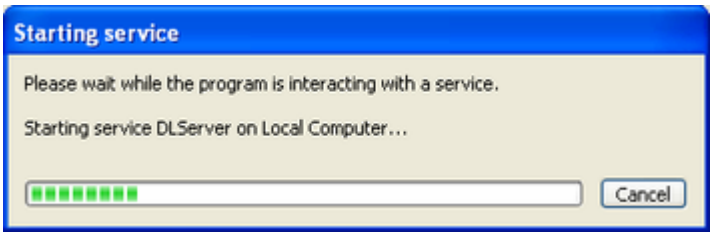
DeviceLock Enterprise Server
The account vm2000ad\test does not belong to the Domain Admins group.
Do you want to continue?
Yes
No

È comunque possibile continuare con la procedura guidata facendo clic sul pulsante **Sì**. In questo caso, è bene tenere presente che l'utente specificato deve possedere i privilegi amministrativi completi per accedere in remoto a tutti i servizi di DeviceLock in esecuzione oppure il certificato di DeviceLock (la chiave pubblica) deve essere installato su ciascun computer su cui è installato DeviceLock Service.

Se si seleziona l'opzione **This account** e l'account utente specificato non dispone del privilegio di sistema Log On As A Service, questo sarà automaticamente assegnato dalla procedura guidata. Questo privilegio è necessario poiché consente all'utente di avviare il servizio.

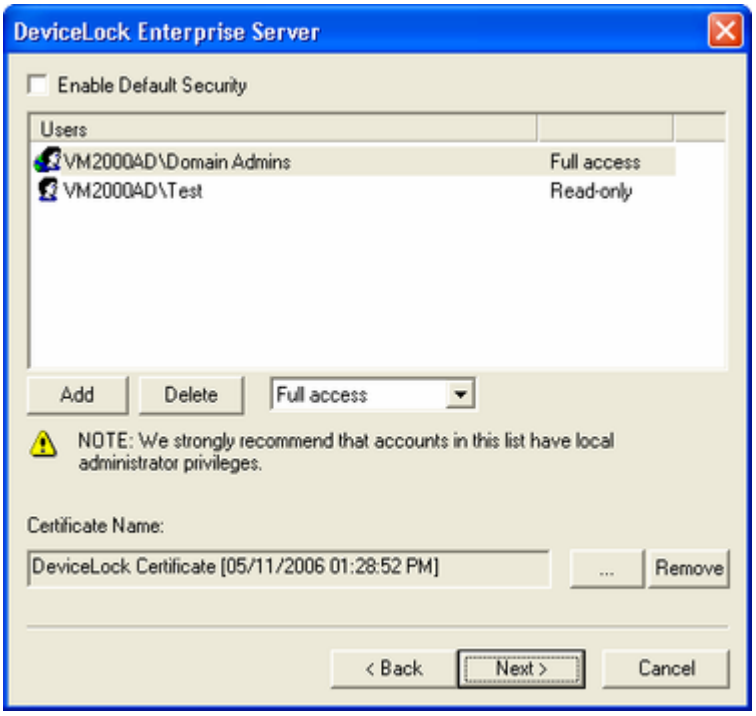


Se tutti i parametri di avvio del servizio sono stati configurati correttamente, la procedura guidata avvierà DeviceLock Enterprise Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLServer on Local Computer...
Cancel

La procedura di avvio del servizio di DeviceLock Enterprise Server e la visualizzazione della pagina successiva della procedura guidata richiedono diverso tempo (fino ad un minuto).

Sulla seconda pagina della procedura guidata, è possibile definire l'elenco degli utenti che dispongono dei privilegi amministrativi per accedere a DeviceLock Enterprise Server e per installare il certificato di DeviceLock (la chiave privata).



Opzione "Enable Default Security"
Se si attiva la configurazione di protezione predefinita, tutti gli utenti che dispongono dei privilegi di amministratore locale, ovvero che sono membri del gruppo locale Administrators, possono connettersi a DeviceLock Enterprise Server tramite una console di gestione per modificarne le impostazioni e per generare i report.

Per attivare la protezione predefinita, selezionare la casella di controllo **Enable Default Security**.

Per definire un accesso a DeviceLock Enterprise Server più granulare, disattivare la protezione predefinita deselezionando la casella di controllo **Enable Default Security**.

Specificare quindi gli account autorizzati (utenti e/o gruppi) che potranno connettersi a DeviceLock Enterprise Server. Per aggiungere un nuovo utente o un gruppo di utenti all'elenco degli account, fare clic sul pulsante **Add**. È possibile aggiungere più account contemporaneamente.

Per eliminare un elemento dall'elenco degli account, selezionarlo e quindi fare clic sul pulsante **Delete**. Per evidenziare ed eliminare più elementi contemporaneamente, utilizzare i tasti Ctrl e/o Maiusc.

Per specificare le azioni consentite ad un utente o ad un gruppo di utenti, impostare le autorizzazioni appropriate:

- **Full access** – consente l'accesso completo a DeviceLock Enterprise Server. Gli utenti possono modificare le impostazioni e avviare i report.
- **Change** – consente l'accesso a DeviceLock Enterprise Server per modificarne le impostazioni. Gli utenti possono modificare le impostazioni, installare/rimuovere DeviceLock Enterprise Server e avviare i report. Gli utenti non possono, invece, aggiungere nuovi elementi all'elenco degli account autorizzati a connettersi a DeviceLock Enterprise Server, né possono cambiare i privilegi di accesso assegnati agli utenti presenti in tale elenco.
- **Read-only** – consente l'accesso a DeviceLock Enterprise Server in sola lettura. Gli utenti possono avviare i report e visualizzare le impostazioni, ma non possono modificare alcun parametro.

Nota: si consiglia caldamente di aggiungere in questo elenco account che dispongano dei privilegi di amministratore locale poiché, in alcuni casi, l'installazione, l'aggiornamento e la disinstallazione del servizio di DeviceLock Enterprise Server richiede i privilegi di accesso a Windows Service Control Manager (SCM) e alle risorse di rete condivise.

Campo "Certificate Name"
Per attivare l'autenticazione basata sul certificato di DeviceLock, è necessario distribuire la chiave privata a DeviceLock Enterprise Server.

Sono disponibili due metodi per autenticare DeviceLock Enterprise Server sui computer remoti che eseguono DeviceLock Service:

- **Autenticazione dell'utente** – t il servizio di DeviceLock Enterprise Server è stato avviato con un account utente che dispone dei privilegi amministrativi

completi per accedere a DeviceLock Service sul computer remoto. Per ulteriori informazioni su come avviare DeviceLock Enterprise Server con un account utente, leggere la sezione Gruppo di opzioni "Log on as".

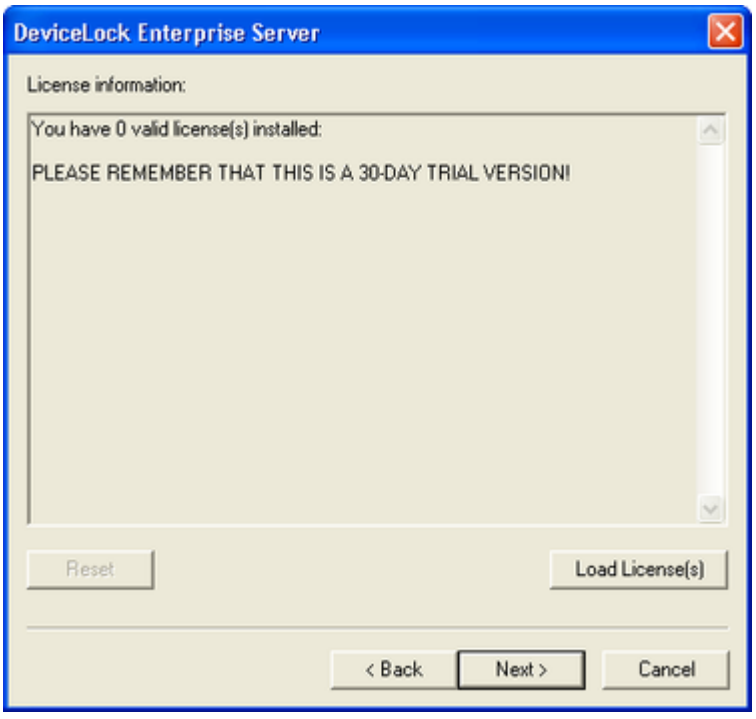
- **Autenticazione basata sul certificato di DeviceLock** – se DeviceLock Enterprise Server è stato avviato con un account utente che non può accedere a DeviceLock Service sul computer remoto, è necessario effettuare l'autenticazione basata sul certificato di DeviceLock.
  La chiave pubblica deve essere installata sul computer che ospita DeviceLock Service e la corrispondente chiave privata deve essere installata sul computer che ospita DeviceLock Enterprise Server.

Per installare il certificato di DeviceLock, fare clic sul pulsante **...**, quindi selezionare un file con chiave privata. Per rimuovere il certificato di DeviceLock, fare clic sul pulsante **Remove**.

Per ulteriori informazioni sul certificato di DeviceLock, leggere la sezione Certificati di DeviceLock.

Fare clic sul pulsante **Next** per applicare le modifiche e visualizzare la terza pagina della procedura di configurazione guida.

In questa pagina è possibile caricare i file delle licenze di DeviceLock.



Sezione "License information"
Se è stata acquistata una licenza per DeviceLock, caricare il relativo file in DeviceLock Enterprise Server.

DeviceLock Enterprise Server gestisce solamente il numero di servizi di DeviceLock licenziati. Ad esempio, se si è in possesso di una licenza valida per 100 computer, ma nella propria rete sono in esecuzione 101 servizi di DeviceLock, DeviceLock Enterprise Server lavorerà solamente con i primi 100 servizi di DeviceLock e ignorerà il servizio rimanente.

Per caricare una licenza, fare clic sul pulsante **Load License(s)** e quindi selezionare il file della licenza.

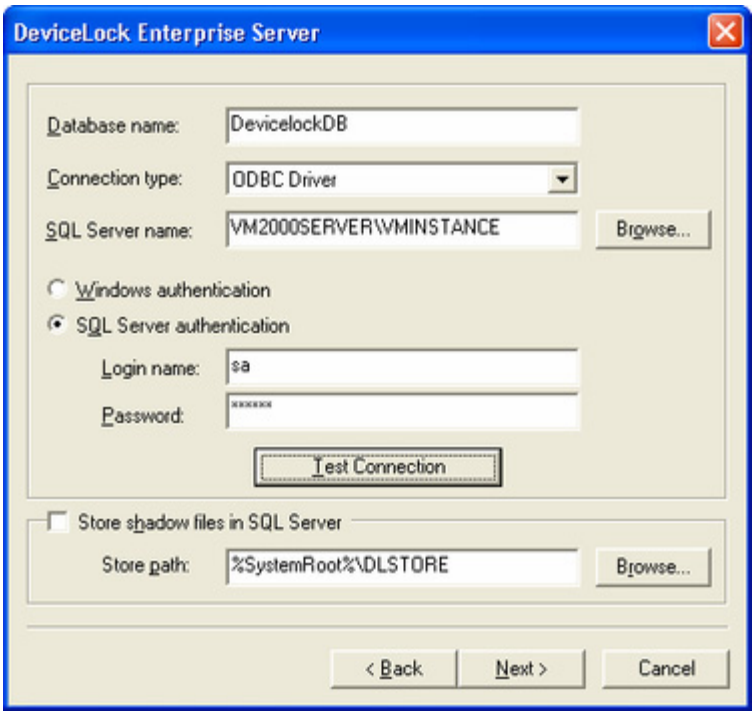
È possibile caricare più file delle licenze in serie - una alla volta.

Se non sono state caricate delle licenze valide, DeviceLock Enterprise Server funzionerà in modalità di valutazione e potrà gestire solamente due servizi di DeviceLock.

Nota: se un computer munito di DeviceLock Service si scollega dalla rete, DeviceLock Enterprise Server si occupa della sostituzione solo dopo un riavvio o dopo sei ore.

Fare clic sul pulsante **Next** per installare le licenze e visualizzare la quarta pagina della procedura guidata.

La quarta pagina consente di configurare i parametri del database.



Campo "Database name"
In questo campo è necessario specificare il nome del database SQL Server in cui DeviceLock Enterprise Server dovrà archiviare i dati. Per impostazione predefinita, il nome del database suggerito dalla procedura guidata è **DeviceLockDB**.

Nota: non occorre creare manualmente un database con il nome pertinente, poiché la procedura di configurazione guidata crea automaticamente il database o utilizza quello esistente.

Campo "Connection type"
Per accedere al database SQL Server sono disponibili due metodi:

1. **ODBC Driver** – se si seleziona questo metodo, specificare nel campo **SQL Server name** il nome del server SQL e quindi selezionare la modalità di autenticazione (Windows oppure SQL Server).

   Nel campo **SQL Server name** è necessario specificare sia il nome del computer su cui SQL Server è in esecuzione, sia il nome SQL Server. Generalmente, il nome SQL Server è costituito da due parti: il nome del computer e il nome dell'istanza separati dal carattere "barra rovesciata" (ad esempio, computer\istanza). A volte, il nome dell'istanza è vuoto (valore predefinito) ed è possibile utilizzare il nome del computer come nome SQL Server. Per ottenere i nomi SQL Server disponibili nella rete locale, fare clic sul pulsante **Browse** (per ottenere il nome dell'istanza, è necessario poter accedere al registro remoto della macchina che ospita SQL Server).

   Se il campo **SQL Server name** è vuoto, vuol dire che SQL Server è in esecuzione sullo stesso computer su cui è installato DeviceLock Enterprise Server. Anche il nome dell'istanza risulta vuoto (valore predefinito).

   Per stabilire una connessione a SQL Server, è necessario configurare anche i parametri di autenticazione.

   Selezionare l'opzione **Windows authentication** per autenticarsi a SQL Server con l'account utente utilizzato per avviare il servizio di DeviceLock Enterprise Server.

   Se il servizio è stato avviato con l'account utente SYSTEM e SQL Server è ospitato su un computer remoto, il servizio non sarà in grado di connettersi a SQL Server poiché l'account utente SYSTEM non dispone dei diritti per accedere alla rete. Per ulteriori informazioni su come avviare DeviceLock Enterprise Server con un account utente, leggere la sezione Gruppo di opzioni "Log on as".

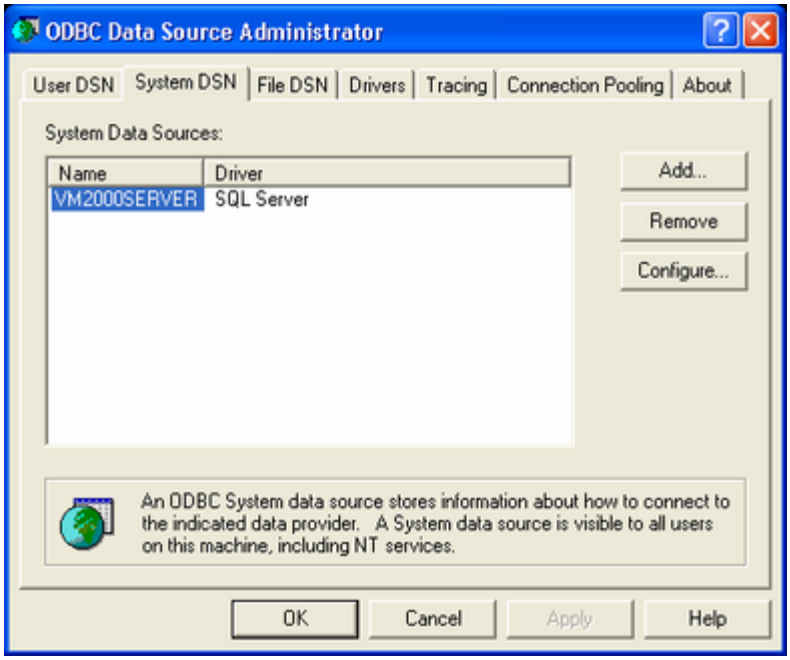
   Selezionare l'opzione **SQL Server authentication** per consentire a SQL Server di effettuare l'autenticazione una volta convalidati il nome utente e la password precedentemente specificati. Prima di selezionare l'opzione **SQL Server authentication**, assicurarsi che SQL Server sia configurato per utilizzare l'autenticazione in modalità mista.

   Immettere il nome utente SQL (login) nel campo **Login name** e la relativa password nel campo **Password**.

Nota: la modalità di autenticazione di Windows garantisce maggiore protezione rispetto alla modalità di autenticazione di SQL Server. Quando è possibile, è consigliabile utilizzare la modalità di autenticazione di Windows.

2. **System Data Source** – seleziona l'origine dati di sistema predefinita dall'elenco **Data Source**.

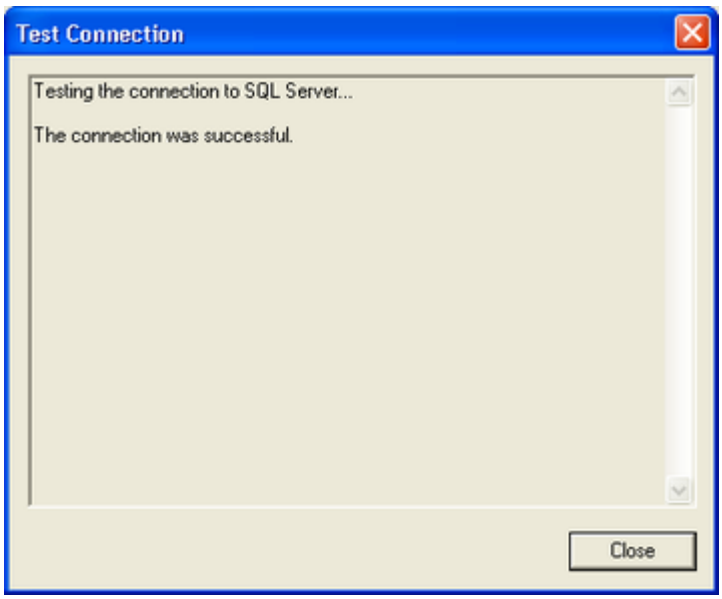
   Per definire le origini dati, utilizzare l'applet **Origine dati (ODBC)**, richiamabile da **Pannello di controllo** -> **Strumenti di amministrazione**.



Se nella configurazione dell'origine dati è stato scelto il metodo di autenticazione di SQL Server, è necessario immettere il nome utente SQL (account di accesso) nel campo **Login name** e la relativa password nel campo **Password**. Se è stato selezionato il metodo di autenticazione di Windows, lasciare questi campi in bianco.

Per aggiornare l'elenco Data Source Name, fare clic sul pulsante **Refresh**.

Una volta definito l'accesso a SQL Server, è possibile eseguire un test di verifica. Fare clic sul pulsante **Test Connection** per assicurarsi che tutti i parametri siano stati configurati correttamente.



Questo test verificherà solamente la connessione ed i propri diritti di accesso a SQL Server. Se si verificano dei problemi con il database o con i diritti di accesso al database, tali problemi non saranno visualizzati nella finestra di dialogo **Test Connection**.

Se sono stati configurati dei parametri di connessione non validi, verrà notificato uno dei seguenti errori:

- **SQL Server does not exist or access denied** – è stato specificato un nome SQL Server non valido nel campo **SQL Server name** oppure il computer remoto che ospita SQL Server non è accessibile. È possibile che sia stato specificato il nome del computer sul quale SQL Server è in esecuzione, ma che non sia stato immesso il nome dell'istanza di SQL Server (ad esempio, computer\istanza).
- **Login failed for user 'COMPUTER_NAME$'** – è stata selezionata la modalità di autenticazione di Windows, ma l'account utente utilizzato per avviare il servizio di DeviceLock Enterprise Server non può accedere al computer che ospita SQL Server. Questo si verifica quando il servizio è stato avviato con l'account utente SYSTEM o con un account utente che non dispone di privilegi amministrativi locali sul computer remoto che ospita SQL Server.
- **Login failed for user 'user_name'** – è stata selezionata la modalità di autenticazione di SQL Server, ma è stato specificato un nome utente SQL (login) non valido oppure è stata immessa una password errata. Gli utenti di SQL differiscono dagli utenti di Windows e non è possibile specificare un nome account regolare di Windows nel campo **Login name**. Gli utenti SQL esistono solamente su SQL Server e, per gestirli, è necessario utilizzare le console di gestione (quali, ad esempio, Microsoft SQL Server e Management Studio).

- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** – è stata selezionata la modalità di autenticazione di SQL Server, ma SQL Server non supporta tale modalità. È necessario utilizzare la modalità di autenticazione di Windows oppure consentire a SQL Server di funzionare in modalità mista (modalità di autenticazione di SQL Server e modalità di autenticazione di Windows).
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** – l'origine dati specificata nel campo **Data Source Name** è stata configurata per utilizzare la modalità di autenticazione di SQL Server ma il parametro **Login name** è vuoto.
- **Data source name not found and no default driver specified** – è stata selezionata l'opzione **System Data Source** dalla casella combinata **Connection type**, ma non è stato specificato alcun nome nel campo **Data Source Name** oppure il nome specificato non è valido.

Opzione "Store shadow files in SQL Server"
I dati binari possono essere memorizzati in un database SQL Server oppure sul disco fisso.

Per memorizzare i dati in un database SQL Server, selezionare la casella di controllo **Store shadow files in SQL Server**.

Se si sceglie di memorizzare i dati binari in un database SQL Server, si consiglia di incrementare in modo sensibile il parametro relativo alla dimensione massima del file di log delle transazioni del database specificato nel campo **Database name**. In caso contrario, SQL Server potrebbe non essere in grado di gestire una grande quantità di dati (centinaia di megabyte) durante una transazione. Si consiglia inoltre di incrementare la quantità massima di memoria disponibile per SQL Server e di attivare la funzionalità PAE (Physical Address Extension - estensione indirizzo fisico).

Per ulteriori informazioni su come configurare SQL Server per ottenere le migliori prestazioni, leggere il seguente articolo disponibile sul sito Web di Microsoft: http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/rdbmspft.mspx.

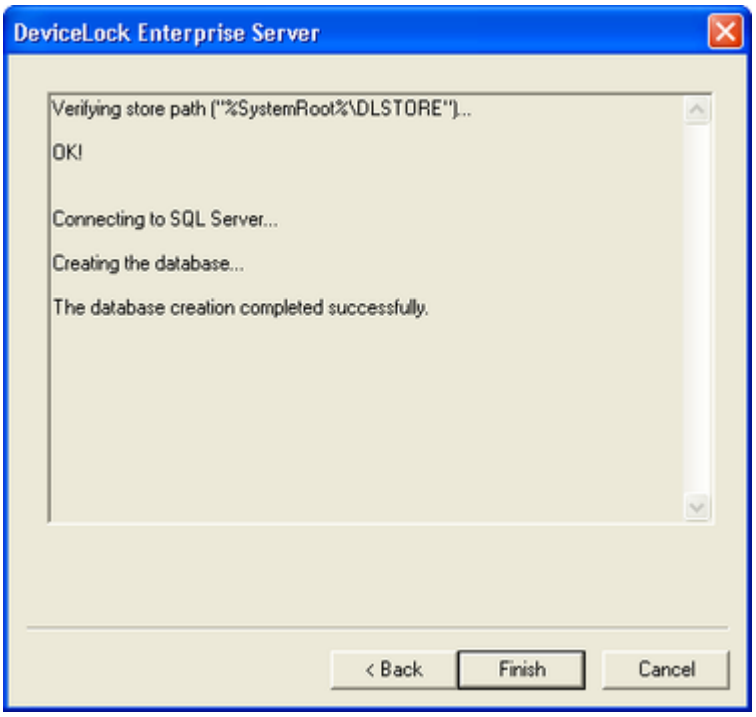
Per memorizzare i dati sul disco, deselezionare la casella di controllo **Store shadow files in SQL Server**. In questo caso, nel database SQL Server vengono memorizzati solamente i collegamenti ai dati ed alcune informazioni addizionali.

I dati vengono memorizzati nel percorso specificato nel campo **Store path**. Per scegliere la cartella in cui archiviare i dati, fare clic sul pulsante **Browse**.

È possibile specificare anche una risorsa di rete condivisa (ad esempio, \\server\dlstore). Assicurarsi che l'account utente utilizzato per avviare il servizio di DeviceLock Enterprise Server disponga dell'accesso completo alla risorsa di rete specificata.

Nota: si consiglia di memorizzare i dati binari sul disco.

Fare clic sul pulsante **Next** per applicare le modifiche e visualizzare l'ultima pagina della procedura guidata.



DeviceLock Enterprise Server procederà alla creazione del database specificato nel campo **Database name** qualora non esista in SQL Server. L'operazione richiederà diverso tempo per essere completata. Se invece il database già esiste ed è stato precedentemente creato da DeviceLock Enterprise Server, DeviceLock Enterprise Server utilizzerà tale database preservando i dati in esso contenuti.

Nota: se necessario, DeviceLock aggiorna automaticamente il database all'ultima versione.

Se sono stati specificati dei parametri non corretti nelle pagine precedenti della procedura guidata, sarà visualizzato uno dei seguenti messaggi di errore:

- **[2] The system cannot find the file specified** – DeviceLock Enterprise Server è stato configurato per memorizzare i dati binari sul disco ma il percorso specificato nel campo **Store path** non è valido. Se è stata specificata una risorsa di rete condivisa, è possibile che la risorsa di rete non sia accessibile.
- **Failed to verify store path. [5] Access is denied** – il percorso specificato nel campo **Store path** è valido, ma l'account utente utilizzato per avviare il servizio di DeviceLock Enterprise Server non dispone dell'accesso completo ai file memorizzati nel percorso.

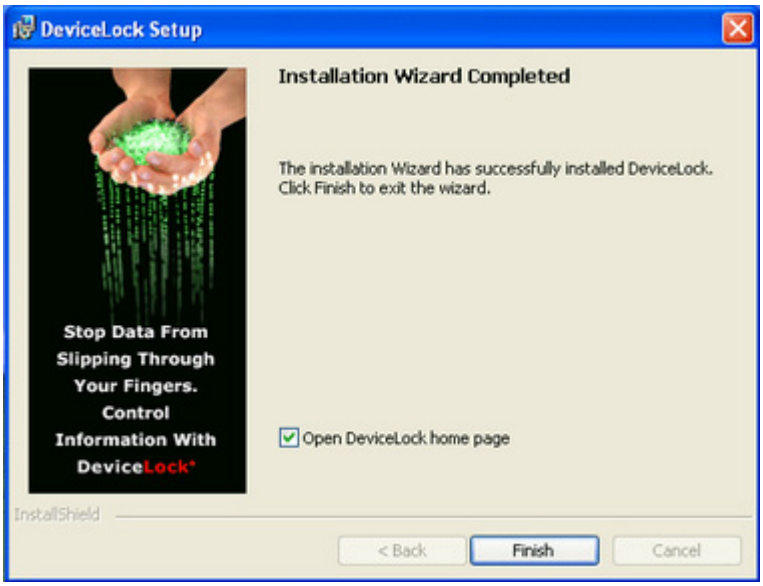
- **CREATE DATABASE permission denied in database 'name'** – l'account utente utilizzato per accedere a SQL Server non dispone di privilegi sufficienti per creare il database. L'account di accesso dovrebbe essere almeno un membro del ruolo predefinito del server dbcreator (vedere **Ruoli del server** nelle **Proprietà di accesso** di Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** – l'account utente utilizzato per accedere a SQL Server non ha accesso al database esistente. L'utente dovrebbe essere mappato ad un account di accesso a questo database (vedere **Mappare un utente** nelle **Proprietà di accesso** di Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** – l'account utente utilizzato per accedere a SQL Server non ha accesso in lettura/scrittura al database esistente. L'account di accesso dovrebbe essere almeno un membro dei ruoli predefiniti del database db_datareader e db_datawriter (vedere **Mappare un utente** nelle **Proprietà di accesso** di Microsoft SQL Server Management Studio).
- **Invalid object name 'name'** – il database specificato nel campo **Database name** già esiste in questo SQL Server ma ha un formato non corretto. Questo si verifica quando si sta tentando di utilizzare un database che non è stato creato con DeviceLock Enterprise Server oppure quando il database è danneggiato.
- **DeviceLock Database has an unsupported format** – il database specificato nel campo **Database name** già esiste ma è vecchio. Questo database ha un formato non supportato e non può essere automaticamente aggiornato al nuovo formato. È necessario utilizzare un database differente oppure crearne uno nuovo.
- **DeviceLock Database has a format that is not supported by the current server version** – il database specificato nel campo **Database name** già esiste ma è stato creato con un versione più recente di DeviceLock Enterprise Server. È necessario utilizzare la versione più recente di DeviceLock Enterprise Server oppure utilizzare un database differente (o crearne uno nuovo).

È possibile che vengano visualizzati anche alcuni messaggi di errore di accesso a SQL Server descritti in precedenza.

Per tornare alla pagina precedente e apportare le modifiche necessarie, fare clic sul pulsante **Back**.

Se non si verificano errori, fare clic sul pulsante **Finish** per chiudere la procedura guidata e continuare la fase di installazione.

Una volta installato DeviceLock, il programma di installazione consiglierà di visitare il sito Web di DeviceLock.



Deselezionare la casella di controllo **Open DeviceLock home page** se non si desidera visitare il sito Web di DeviceLock. Fare clic su **Finish** per terminare l'installazione.

Nota: per disinstallare DeviceLock, eseguire una delle seguenti azioni:

Aprire **Installazione applicazioni** nel Pannello di controllo per rimuovere **DeviceLock**.
- OPPURE -
Fare clic su **Start**, selezionare **Tutti i programmi**, **DeviceLock**, quindi fare clic su **Remove DeviceLock**.

Installazione di DeviceLock Content Security Server

Per installare DeviceLock Content Security Server, attenersi alle seguenti istruzioni:

- Passaggio 1. Preparazione all'installazione
- Passaggio 2. Avvio dell'installazione
- Passaggio 3. Configurazione di DeviceLock Content Security Server e completamento dell'installazione.

Passaggio 1. Preparazione all'installazione

Prima di installare DeviceLock Content Security Server, considerare quanto segue:

- Il computer su cui viene installato DeviceLock Content Security Server deve soddisfare i seguenti requisiti di sistema:

Sistema operativo	Microsoft Windows NT 4.0 Service Pack (SP) 6, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista o Windows 7. L'installazione può essere eseguita indistintamente sulle edizioni a 32 bit e 64 bit del sistema operativo.
Browser Web	Sui computer con sistema operativo Windows NT 4.0 SP 6 deve essere installato Windows Internet Explorer 4.0 o versioni successive.
Spazio libero sul disco rigido	19 MB

- Per installare DeviceLock Content Security Server, è necessario disporre delle autorizzazioni di amministratore.
- Per assicurare prestazioni e affidabilità ottimali, si consiglia di installare DeviceLock Enterprise Server e DeviceLock Content Security Server su computer diversi.
- È necessario acquistare una licenza speciale di Search Server per DeviceLock Content Security Server. È possibile utilizzare la stessa licenza su un numero illimitato di computer in cui viene eseguito DeviceLock Content Security Server. Il modello di licenza di Search Server si basa sul numero di voci di registro da indicizzare per la ricerca full-text. Ogni licenza consente a Search Server di indicizzare 1.000 voci dai registri shadowing (Shadow Log e Deleted Shadow Log) e 5000 voci da ogni altro registro (Audit Log, Server Log e Monitoring Log). A seconda del numero di voci di registro sui DeviceLock Enterprise Server in uso, è possibile acquistare le licenze necessarie. Se si utilizzano più licenze per Search Server, è possibile indicizzare il numero di voci di registro consentito dalle licenze combinate. Il periodo di prova di DeviceLock Content Security Server è di 30 giorni. Durante il periodo di prova, Search Server può indicizzare 2.000 voci dai registri shadowing e 10.000 voci da ogni altro registro.
- Se si dispone di più DeviceLock Enterprise Server nella propria rete, è possibile installare più DeviceLock Content Security Server per distribuire il carico di lavoro. Tuttavia, un approccio del genere è consigliabile solo se i DeviceLock Enterprise Server non sono collegati allo stesso Microsoft SQL Server (vale a dire se non è presente una relazione di tipo "molti-a-uno").
- Se sono installati più DeviceLock Content Security Server, ciascun Search Server dispone del proprio indice di ricerca. Di conseguenza, è necessario collegarsi a ciascun DeviceLock Content Security Server e avviare le stesse query di ricerca su ciascun Search Server per ottenere i risultati completi da tutti i dati memorizzati su tutti i DeviceLock Enterprise Server.
- Si consiglia di chiudere tutti i programmi di Windows prima di avviare l'installazione.

Passaggio 2. Avvio dell'installazione

Seguire questa procedura per avviare il programma di installazione.

Per avviare l'installazione

1. Aprire il file **DeviceLock.zip** e fare doppio clic sul file **setup_dlcss.exe** per avviare il programma di installazione.

   È necessario avviare il programma di installazione su ciascun computer su cui si desidera installare DeviceLock Content Security Server.

2. Seguire le istruzioni visualizzate sul programma di installazione.
3. Nella pagina **License Agreement**, leggere il contratto di licenza e fare clic su **I accept the terms in the license agreement** per accettare i termini e le condizioni della licenza e procedere con l'installazione.
4. Nella pagina **Customer Information**, digitare il proprio nome utente e il nome dell'organizzazione e fare clic su **Next**.
5. Nella pagina **Destination Folder**, accettare il percorso di installazione predefinito o fare clic su **Change** per scegliere il percorso desiderato. Fare clic su **Next**.

   La directory di installazione predefinita è %ProgramFiles%\DeviceLock Content Security Server.

6. Nella pagina **Ready to Install the Program**, fare clic su **Install** per avviare l'installazione.

   Viene avviata la configurazione guidata di DeviceLock Content.

   Se si sta installando un aggiornamento o si sta reinstallando DeviceLock Content Security Server e si desidera mantenere la configurazione corrente, non è necessario ripetere la configurazione guidata, ma è sufficiente fare clic su **Cancel** per uscire da quest'ultima e mantenere invariate le impostazioni.

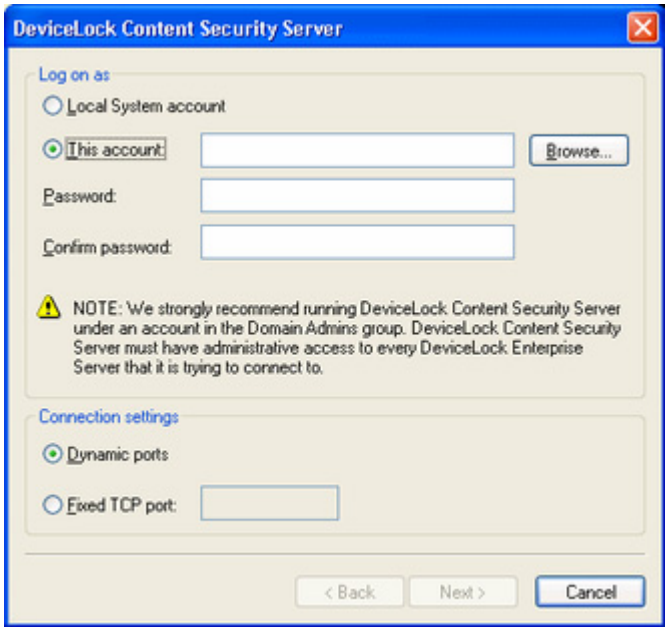
   Se si desidera modificare alcuni parametri e mantenerne altri, cambiare solo i parametri necessari e seguire la configurazione guidata fino alla pressione del pulsante **Finish** nella pagina finale.

   Nota: se DeviceLock Content Security Server viene installato per la prima volta (non sono presenti impostazioni sul computer) e si chiude la configurazione guidata, il programma di installazione non è in grado di installare il servizio DeviceLock Content Security Server e, di conseguenza, è necessario riavviare la configurazione guidata.

Passaggio 3. Configurazione di DeviceLock Content Security Server e completamento dell'installazione

La configurazione guidata di DeviceLock Content Security Server si apre automaticamente durante l'installazione. La procedura suggerisce le impostazioni richieste per l'utilizzo di DeviceLock Content Security Server.

La prima pagina della configurazione guidata ha l'aspetto seguente:


DeviceLock Content Security Server
Log on as
Local System account
This account:
Browse...
Password:
Confirm password:
NOTE: We strongly recommend running DeviceLock Content Security Server under an account in the Domain Admins group. DeviceLock Content Security Server must have administrative access to every DeviceLock Enterprise Server that it is trying to connect to.
Connection settings
Dynamic ports
Fixed TCP port:
< Back
Next >
Cancel

In questa pagina vengono configurate le opzioni di avvio del servizio DeviceLock Content Security Server.

Log on as
Prima di tutto, occorre scegliere un account con cui avviare il servizio DeviceLock Content Security Server. Come succede con numerosi altri servizi Windows, il servizio DeviceLock Content Security Server può essere avviato con l'account di sistema locale speciale (utente SYSTEM) e per conto di qualsiasi utente.

Per avviare il servizio con l'utente SYSTEM, selezionare l'opzione **Local System account**. Tenere presente che il processo che utilizza l'utente SYSTEM non può accedere alle risorse di rete condivise ed effettua l'autenticazione sui computer remoti come utente anonimo. Di conseguenza, se DeviceLock Content Security Server è configurato per l'avvio con l'utente SYSTEM, non può accedere a DeviceLock Enterprise Server in esecuzione sul computer remoto e deve ricorrere al certificato DeviceLock Certificate per eseguire l'autenticazione sul computer.

Per ulteriori informazioni sui metodi di autenticazione, leggere la descrizione del parametro Certificate Name.

Per avviare il servizio per conto dell'utente, selezionare l'opzione **This account** e immettere il nome dell'account e la password. Si consiglia di utilizzare un account utente dotato di privilegi amministrativi su tutti i computer in cui viene eseguito DeviceLock Enterprise Server. In caso contrario, è necessario ricorrere all'autenticazione tramite il certificato di DeviceLock.

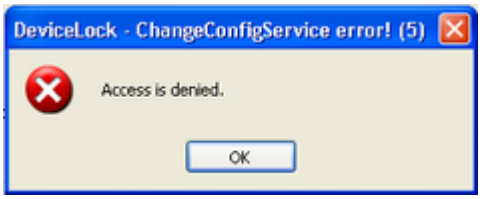
Se DeviceLock Content Security Server viene installato in un ambiente di dominio, si consiglia di utilizzare un account utente appartenente al gruppo di amministratori di dominio. Poiché il gruppo di amministratori di dominio fa parte del gruppo di amministratori locali su tutti i computer del dominio, i membri del gruppo di amministratori di dominio dispongono dell'accesso completo a DeviceLock Enterprise Server su tutti i computer.

Inoltre, se l'opzione della protezione predefinita (Default Security) è disattivata sul DeviceLock Enterprise Server in esecuzione remota, l'account utente specificato nell'opzione **This account** deve essere presente nell'elenco degli amministratori di server con almeno i diritti di accesso **di sola lettura** sul DeviceLock Enterprise Server in questione. In caso contrario, è necessario ricorrere all'autenticazione tramite il certificato di DeviceLock.

Connection settings
È possibile impostare DeviceLock Content Security Server in modo tale da utilizzare una porta TCP fissa per le comunicazioni con la console di gestione, facilitando in tal modo la configurazione del firewall. Digitare il numero della porta nel campo **Fixed TCP port**. Per utilizzare le porte dinamiche per la comunicazione RPC, selezionare l'opzione **Dynamic ports**. Per impostazione predefinita, DeviceLock Content Security Server utilizza la porta 9134.

Fare clic su **Next** per avviare il servizio DeviceLock Content Security Server e passare alla seconda pagina.

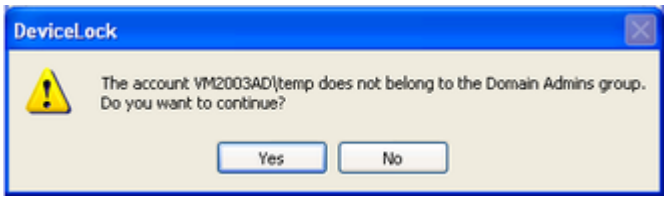
Se l'utente corrente non dispone di un accesso amministrativo completo a DeviceLock Content Security Server (se quest'ultimo è già installato e viene installato un aggiornamento), la configurazione guidata non è in grado di installare il servizio né di applicare le modifiche. Un errore simile può verificarsi se l'utente corrente non dispone dei privilegi amministrativi locali sul computer in cui viene installato DeviceLock Content Security Server.



Se viene specificato un nome utente incorretto o una password errata nell'opzione **This account**, non è possibile avviare DeviceLock Content Security Server.

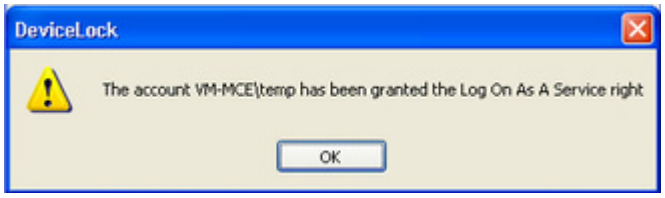
DeviceLock - ChangeConfigService error! (1057)
The account name is invalid or does not exist, or the password is invalid for the account name specified.
OK

Viene visualizzato un messaggio che comunica che l'account utente specificato nell'opzione **This account** non appartiene al gruppo di amministratori di dominio.

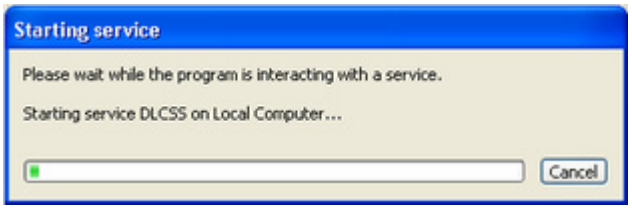


È possibile continuare facendo clic su **Yes**. Tuttavia, in tal caso, se l'utente specificato non dispone dell'accesso amministrativo a tutti i DeviceLock Enterprise Server in esecuzione remota, è necessario installare il certificato di DeviceLock (la chiave privata) su ogni computer in cui è installato DeviceLock Enterprise Server.

Se l'account utente specificato nell'opzione **This account** non dispone del privilegio di sistema Assegna come servizio, il privilegio viene assegnato automaticamente dalla configurazione guidata. È necessario disporre di tale privilegio per avviare il servizio per conto dell'utente.

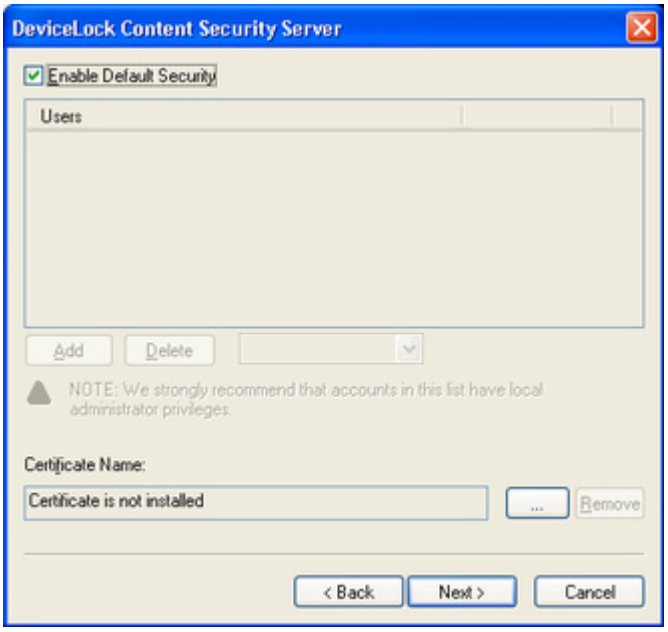


Se tutti i parametri di avvio del servizio sono stati specificati correttamente, la configurazione guidata avvia DeviceLock Content Security Server.


Starting service
Please wait while the program is interacting with a service.
Starting service DLCSS on Local Computer...
Cancel

È necessario attendere circa un minuto prima che il servizio DeviceLock Content Security Server si avvii e venga visualizzata la seconda pagina della configurazione guidata.

La seconda pagina della configurazione guidata ha l'aspetto seguente:



In questa pagina viene definito l'elenco di utenti che dispongono dell'accesso amministrativo a DeviceLock Content Security Server e viene installato il certificato di DeviceLock Certificate (la chiave privata).

Enable Default Security
Nella configurazione di protezione predefinita, tutti gli utenti dotati di privilegi di amministratore locale (vale a dire i membri del gruppo locale degli amministratori) possono collegarsi a DeviceLock Content Security Server utilizzando una console di gestione, modificarne le impostazioni e inoltrare query di ricerca.

Per attivare la protezione predefinita, selezionare la casella di controllo **Enable Default Security**.

Se si desidera definire un accesso più granulare a DeviceLock Content Security Server, disattivare la protezione predefinita deselezionando la casella di controllo **Enable Default Security**.

In seguito, è necessario specificare gli account autorizzati (utenti e/o gruppi) che possono collegarsi a DeviceLock Content Security Server. Per aggiungere un nuovo utente o gruppo all'elenco degli account, fare clic su **Add**. È possibile aggiungere più account simultaneamente.

Per eliminare un record dall'elenco degli account, premere il pulsante **Delete**. È possibile evidenziare e rimuovere più record simultaneamente utilizzando il tasto CTRL o MAIUSC.

Per definire le azioni autorizzate per un utente o un gruppo di utenti, impostare i diritti appropriati:

- **Full access**: attiva l'accesso completo a DeviceLock Content Security Server. Gli utenti possono modificare le impostazioni e inoltrare query di ricerca.
- **Change**: attiva l'accesso a DeviceLock Content Security Server con possibilità di modifica. Gli utenti possono modificare le impostazioni, installare e disinstallare DeviceLock Content Security Server e inoltrare query di ricerca, ma non possono aggiungere nuovi utenti all'elenco degli account autorizzati a collegarsi a DeviceLock Content Security Server né modificare i diritti di accesso degli utenti presenti nell'elenco.
- **Read-only**: attiva l'accesso di sola lettura a DeviceLock Content Security Server. Gli utenti possono inoltrare query di ricerca e visualizzare le impostazioni, ma non possono modificare alcun parametro né creare un nuovo indice per Search Server.

Nota: si consiglia di includere nell'elenco gli account con privilegi di amministratore locale poiché, in alcune istanze, l'installazione, l'aggiornamento e la disinstallazione del servizio DeviceLock Content Security Server può richiedere i diritti di accesso a Gestione controllo servizi di Windows e alle risorse di rete condivise.

Certificate Name
Può essere necessario utilizzare la chiave privata su DeviceLock Content Security Server per attivare l'autenticazione basata sul certificato di DeviceLock.

Sono disponibili due metodi per autenticare DeviceLock Content Security Server su un DeviceLock Enterprise Server in esecuzione remota:

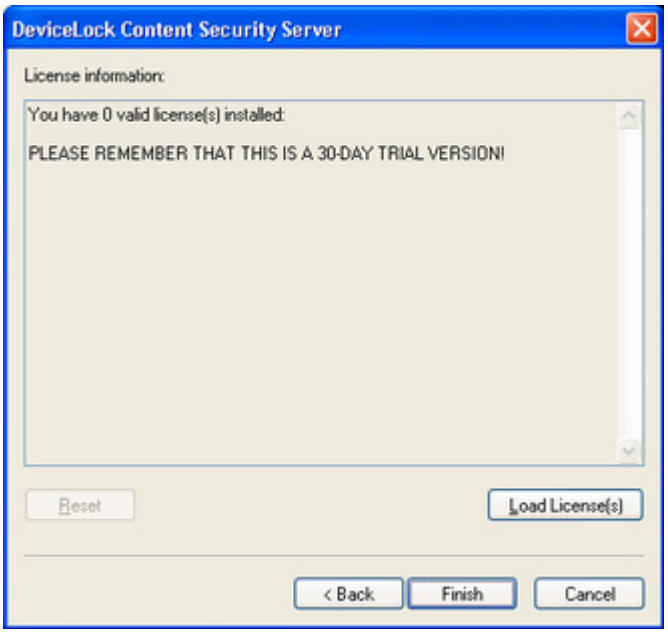
- **Autenticazione utente**: il servizio DeviceLock Content Security Server viene eseguito dall'account utente munito di accesso amministrativo a DeviceLock Enterprise Server sul computer remoto. Per ulteriori informazioni sull'esecuzione di DeviceLock Content Security Server per conto dell'utente, leggere la descrizione del parametro Log on as.
- **Autenticazione tramite certificato di DeviceLock**: se l'utente che esegue DeviceLock Content Security Server non può accedere a DeviceLock Enterprise Server sul computer remoto, occorre eseguire l'autenticazione tramite il certificato di DeviceLock.
  La stessa chiave privata deve essere installata su DeviceLock Enterprise Server e DeviceLock Content Security Server.

Per installare il certificato di DeviceLock, fare clic sul pulsante dei puntini di sospensione e selezionare il file con la chiave privata. Per rimuovere il certificato di DeviceLock, fare clic su **Remove**.

Per ulteriori informazioni sul certificato di DeviceLock, consultare la sezione "Certificati di DeviceLock".

Fare clic su **Next** per applicare le modifiche e passare alla pagina finale della configurazione guidata.

L'ultima pagina della configurazione guidata ha l'aspetto seguente:



In questa pagina è possibile caricare le licenze di DeviceLock Content Security Server.

License information
Se è stata acquistata una licenza per Search Server, è necessaria caricarla in DeviceLock Content Security Server.

Per caricare la licenza, fare clic su **Load License(s)** e selezionare il file della licenza. È possibile caricare più file di licenza, uno alla volta.

Il periodo di prova di DeviceLock Content Security Server è di 30 giorni.

Fare clic su **Finish** per chiudere la configurazione guidata e proseguire con il processo di installazione. In seguito, nella pagina **Installation Wizard Completed**, fare clic su **Finish** per completare l'installazione. Da questa pagina è possibile accedere alla pagina principale di DeviceLock Content Security Server. Questa opzione è selezionata per impostazione predefinita.

Nota: per disinstallare DeviceLock Content Security Server, eseguire una delle seguenti azioni:

Aprire **Installazione applicazioni** nel Pannello di controllo per rimuovere **DeviceLock Content Security Server**.
- OPPURE -

Fare clic su **Start**, selezionare **Tutti i programmi**, **DeviceLock**, quindi fare clic su **Remove DeviceLock Content Security Server**.

Certificati di DeviceLock

Informazioni generali

Il certificato di DeviceLock è un certificato crittografato composto da una chiave privata e da una chiave pubblica.

- La chiave privata deve essere memorizzata sul computer dell'amministratore e solo l'amministratore deve essere in grado di accedervi. La chiave privata deve essere installata anche sul computer che ospita DeviceLock Enterprise Server e DeviceLock Content Security Server.

  Nota: assicurarsi che gli utenti standard non possano accedere alla chiave privata.

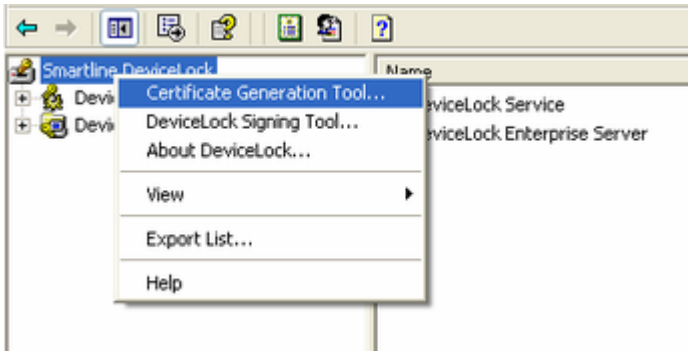
- La chiave pubblica viene installata su tutti i computer che eseguono DeviceLock Service. Se la chiave pubblica non viene installata sul computer dell'utente, non sarà possibile utilizzare la funzione Temporary White List oppure non sarà possibile effettuare l'autenticazione a DeviceLock Enterprise Server tramite il certificato di DeviceLock.

Creazione dei certificati di DeviceLock

Lo strumento Certificate Generation di DeviceLock consente di creare i certificati di DeviceLock.

Si consiglia di creare un solo certificato di DeviceLock e di distribuire la relativa chiave pubblica a tutti i computer degli utenti. È necessario creare e installare un nuovo certificato solamente quando la chiave privata è stata compromessa (ad esempio, è stata rubata) oppure è stata smarrita.

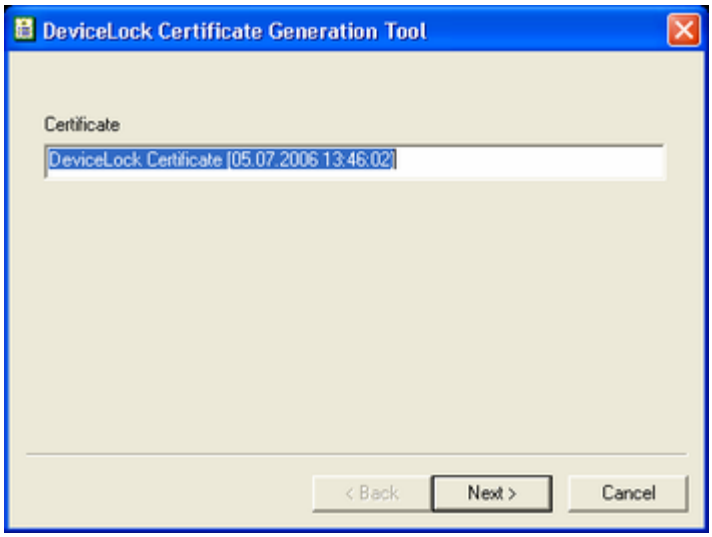
Per avviare lo strumento Certificate Generation, selezionare **Certificate Generation Tool** dal menu **File** in DeviceLock Enterprise Manager. Per avviare lo strumento Certificate Generation da DeviceLock Management Console (lo snap-in MMC) e DeviceLock Group Policy Manager, utilizzare il menu contestuale richiamabile facendo clic con il pulsante destro del mouse.



Lo strumento Certificate Generation viene automaticamente avviato quando le console di gestione di DeviceLock vengono installate su un computer dell'amministratore che non dispone del certificato di DeviceLock.

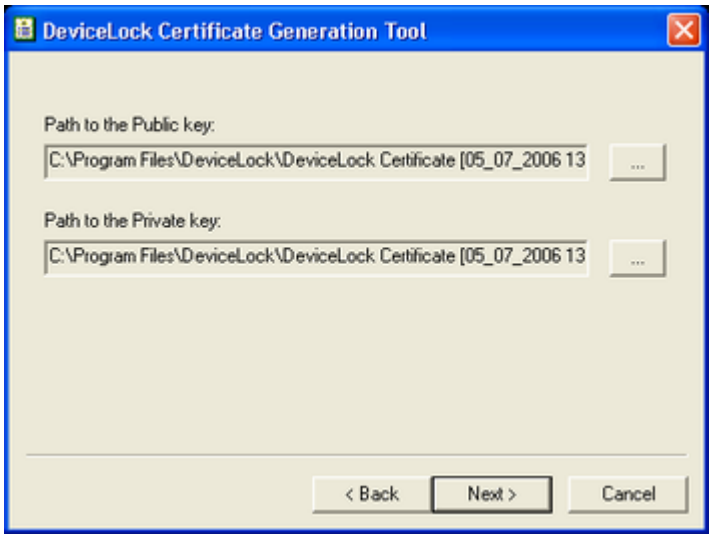
Per generare la coppia di chiavi, è sufficiente eseguire due semplici passaggi:

1. Definire il nome del certificato di DeviceLock.



Lo strumento Certificate Generation propone automaticamente un nome, basato sulla data e sull'ora correnti, ma è possibile scegliere un qualsiasi altro nome.

2. Specificare il percorso e i nomi dei file della chiave privata e della chiave pubblica.



Non appena la creazione del certificato di DeviceLock è stata completata, sarà possibile distribuire la chiave pubblica ai computer degli utenti.

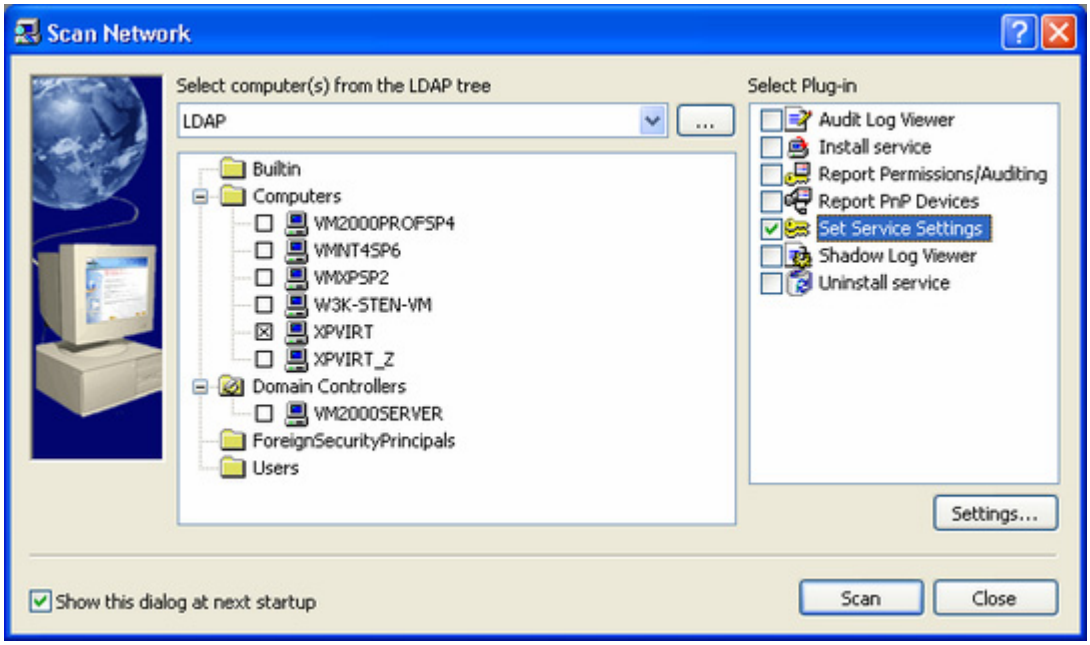
Nota: lo strumento Certificate Generation di DeviceLock non installa automaticamente il certificato appena creato sui computer degli utenti. È necessario distribuire manualmente il certificato di DeviceLock utilizzando una delle console di gestione di DeviceLock.

Installazione/rimozione del certificato di DeviceLock

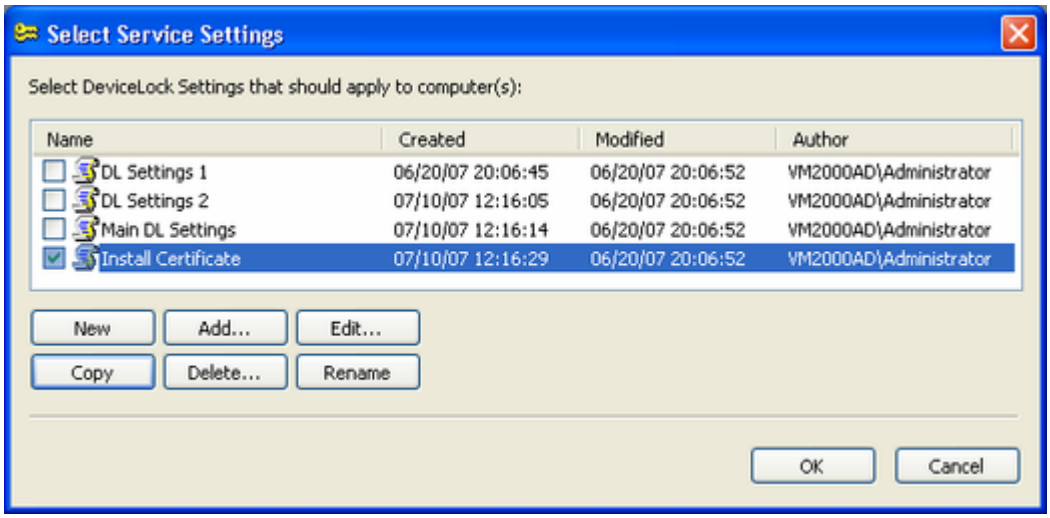
Per installare/rimuovere la chiave pubblica sui/dai computer che eseguono DeviceLock Service, è possibile utilizzare la console di gestione di DeviceLock.

- DeviceLock Enterprise Manager

  Nella finestra di dialogo **Scan Network**, selezionare i computer su cui effettuare l'operazione di installazione/rimozione della chiave pubblica e quindi selezionare il plug-in **Set Service Settings**.



  Fare clic sul pulsante **Settings** oppure fare doppio clic sul plug-in per aprire la finestra di configurazione.

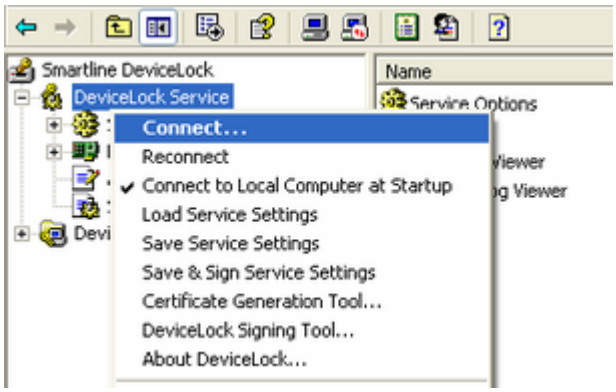


Creare il nuovo file XML o utilizzare quello esistente per definire il criterio necessario per installare/rimuovere il certificato. Selezionare il file nell'elenco e fare clic sul pulsante **Edit** per modificare il criterio come descritto nella sezione successiva. Una volta modificato il criterio, selezionare il file corrispondente spuntando la casella di controllo posta accanto al nome del file nell'elenco.

Fare clic sul pulsante **OK** per chiudere la finestra di configurazione e quindi scegliere **Scan** nella finestra di dialogo **Scan Network** per installare/rimuovere il certificato di DeviceLock.

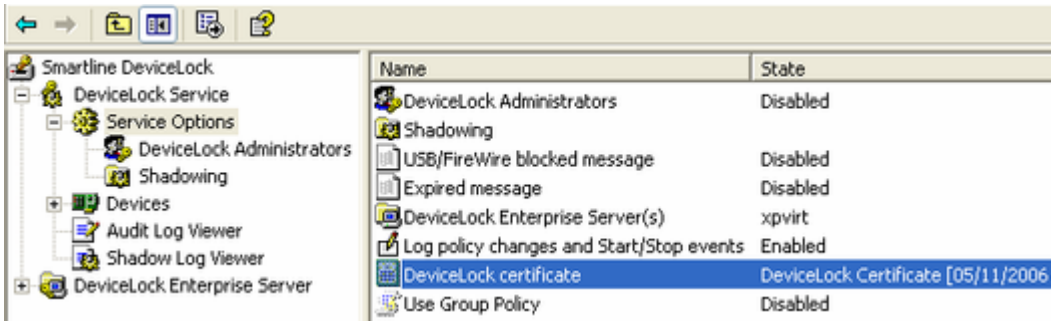
- DeviceLock Management Console, DeviceLock Group Policy Manager and DeviceLock Service Settings Editor

  Se si sta utilizzando DeviceLock Management Console (lo snap-in MMC), fare clic con il pulsante destro del mouse e connettere la console al computer su cui è in esecuzione DeviceLock Service.



Se si utilizza DeviceLock Group Policy Manager, non è necessario connettersi ad un computer poiché si è già connessi all'oggetto Criteri di gruppo. Inoltre, non è necessario connettersi al computer quando si modifica il criterio nel file XML utilizzando DeviceLock Service Settings Editor.

Selezionare **Service Options**.



Fare doppio clic sulla voce **DeviceLock certificate** per aprire la finestra di configurazione.

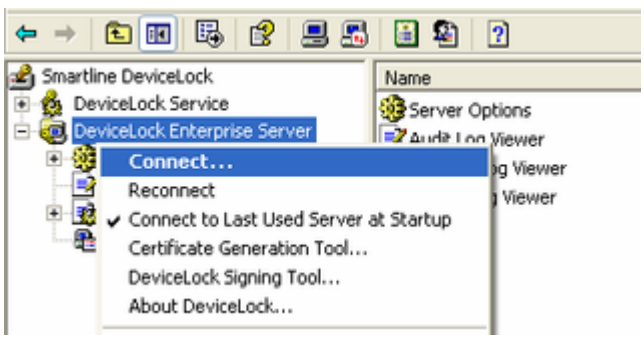
Se si desidera installare il certificato, specificare il percorso della chiave pubblica nel campo **Certificate Name**. Per selezionare il file della chiave pubblica, fare clic sul pulsante **...**.

Per rimuovere la chiave pubblica, fare clic sul pulsante **Remove**.

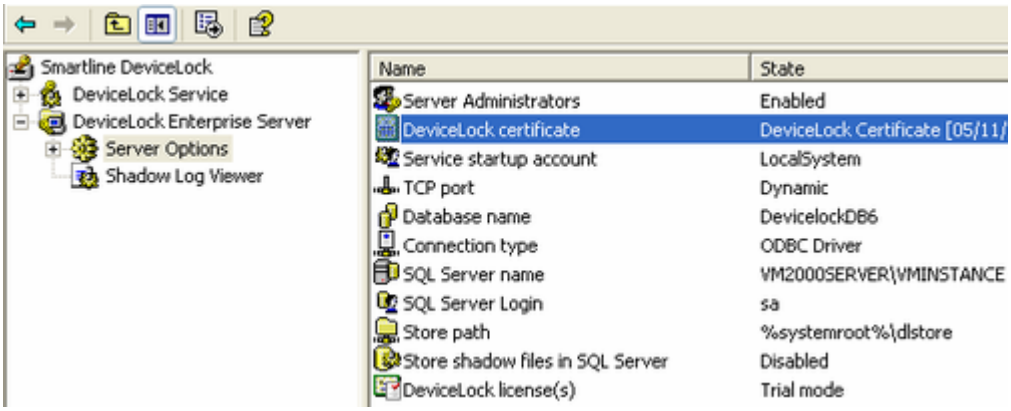
Fare clic sul pulsante **OK** per chiudere la finestra di configurazione ed applicare le modifiche.

Per installare/rimuovere la chiave privata su/da DeviceLock Enterprise Server e DeviceLock Content Security Server, è possibile utilizzare DeviceLock Management Console (lo snap-in MMC).

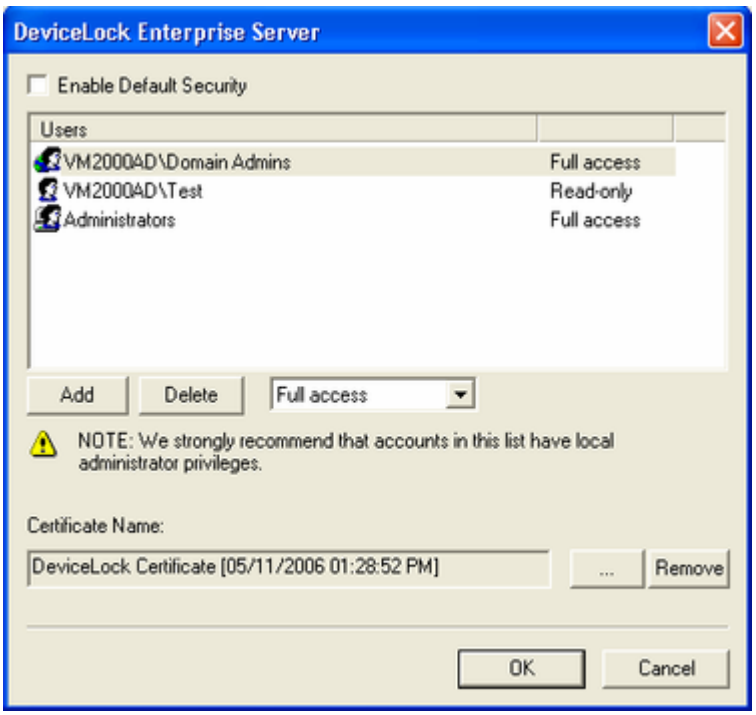
Fare clic con il pulsante destro del mouse e connettere DeviceLock Management Console al computer che esegue DeviceLock Enterprise Server DeviceLock o Content Security Server. Usare il menu contestuale visualizzato facendo clic con il pulsante destro del mouse.



Selezionare **Server Options**.



Fare doppio clic su **DeviceLock certificate** per aprire la finestra di configurazione.



Per installare il certificato, specificare il percorso della chiave privata nel campo **Certificate Name**. Per selezionare il file della chiave privata, fare clic sul pulsante **...**.

Per rimuovere la chiave privata, fare clic sul pulsante **Remove**.

Fare clic sul pulsante **OK** per chiudere la finestra di configurazione ed applicare le modifiche.

Per ulteriori informazioni relative all'installazione della chiave privata su DeviceLock Enterprise Server e DeviceLock Content Security Server, leggere le sezioni

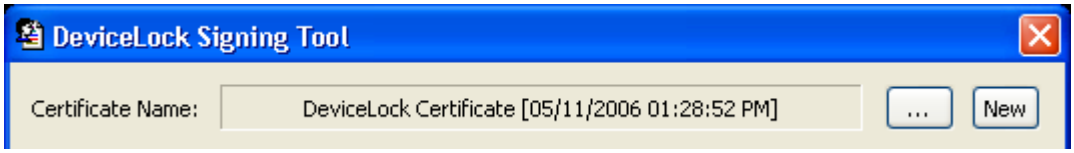
Installazione di DeviceLock Enterprise Server e Installazione di DeviceLock Content Security Server del presente manuale.

Strumento DeviceLock Signing

Informazioni generali

Lo strumento DeviceLock Signing consente agli utenti di accedere temporaneamente alle periferiche richieste e firma i file XML in cui sono memorizzate le impostazioni di DeviceLock Service esportate da DeviceLock Management Console o DeviceLock Group Policy Manager.

Per avviare DeviceLock Signing, selezionare **DeviceLock Signing Tool** dal menu **File** in DeviceLock Enterprise Manager oppure dal menu contestuale di DeviceLock Management Console (lo snap-in MMC), DeviceLock Group Policy Manager o DeviceLock Service Settings Editor.



Innanzitutto, è necessario caricare il corrispondente certificato di DeviceLock (la chiave privata).

La chiave privata deve appartenere allo stesso certificato a cui appartiene la chiave pubblica installata sul computer dell'utente.

Per impostazione predefinita, DeviceLock Signing carica automaticamente l'ultimo certificato utilizzato. Per caricare un certificato differente, fare clic sul pulsante **...** e selezionare il file con la chiave privata.

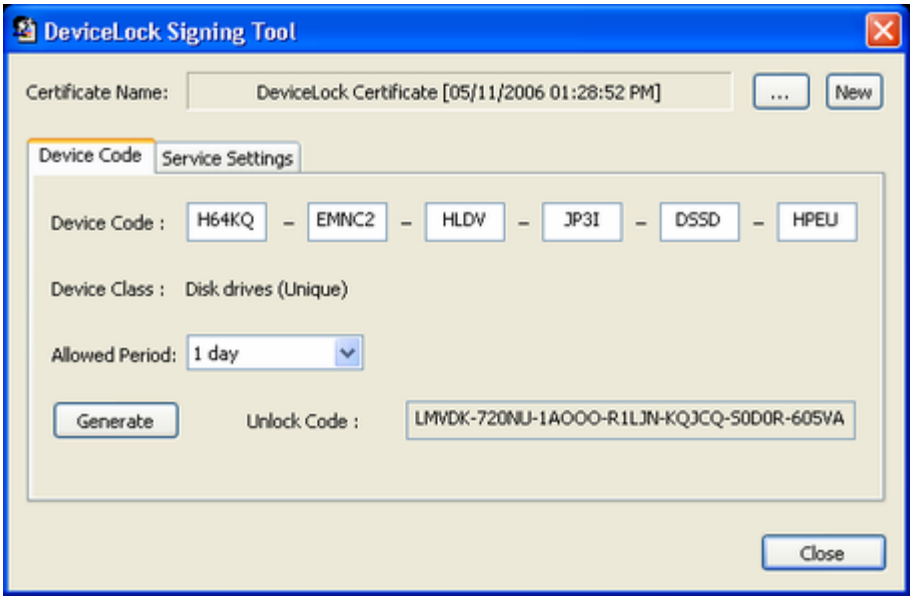
Se si desidera creare un nuovo certificato, fare clic sul pulsante **New** per avviare lo strumento Certificate Generation direttamente da DeviceLock Signing. È bene notare che se si genera un nuovo certificato e si intende utilizzare la relativa chiave privata in DeviceLock Signing, è necessario distribuire la corrispondente chiave pubblica sul computer dell'utente.

Successivamente, è possibile decidere se generare un Codice di sblocco (Unlock Code) oppure se firmare un file XML in cui sono memorizzate le impostazioni di DeviceLock Service.

Codice periferica (Device Code)

Per consentire ad un utente di accedere temporaneamente alla periferica richiesta, è necessario creare un codice di sblocco (Unlock Code) in base al codice periferica (Device Code) ricevuto dall'utente.

Per ulteriori informazioni sull'utilizzo di una white list temporanea, leggere la sezione Temporary White List.



Per creare un codice di sblocco (Unlock Code) da assegnare all'utente, è sufficiente eseguire quattro semplici passaggi:

1. Caricare il corrispondente certificato di DeviceLock (vedere qui).
2. Immettere il codice periferica (Device Code) fornito dall'utente.

   Una volta immesso il codice periferica corretto, nel campo **Device Class** è possibile vedere la classe di appartenenza della periferica a cui l'utente vuole accedere. Le informazioni fornite sulla classe di appartenenza della periferica sono utili per verificare il tipo di periferica che l'utente ha intenzione di utilizzare. Ad esempio, se l'utente avvisa l'amministratore che intende utilizzare uno scanner USB ed invece sta tentando di accedere ad una unità flash USB, l'amministratore è in grado di rilevare immediatamente l'incongruità della richiesta.

   Inoltre, le informazioni racchiuse tra parentesi tonde specificano se la periferica richiesta può essere autorizzata come periferica univoca (**Unique**) o come modello (**Model**), ovvero se la periferica dispone o meno di un numero di serie. Se si autorizza la periferica come modello, l'utente potrà accedere a tutte le periferiche appartenenti a quel determinato modello. Per ulteriori informazioni su questo argomento, leggere la sezione White List delle periferiche USB.

3. Specificare il periodo di tempo in cui l'utente è autorizzato ad accedere alla periferica richiesta. Nella casella **Allowed Period**, è possibile selezionare diversi periodi predefiniti (5, 15, 30 e 60 minuti, 5 ore, 1 o 2 giorni, 1 o 2 settimane, 1 mese, fino a quando la periferica non viene scollegata o fino a quando l'utente non si scollega).

   Se si sceglie un periodo di tempo fisso (ad esempio, 10 minuti), l'utente potrà accedere alla periferica richiesta solo per il periodo di tempo impostato. Una

volta scaduto il periodo, l'accesso alla periferica viene nuovamente negato e le eventuali operazioni correntemente effettuate dall'utente sulla periferica vengono forzatamente interrotte, anche se è in corso la copia dei file su un disco USB o la stampa di un documento su una stampante USB.

Per consentire l'accesso alla periferica richiesta senza limiti di tempo, scegliere until unplug dalla casella combinata **Allowed Period**. L'utente potrà così accedere alla periferica fintanto che rimane collegata alla porta. Non appena l'utente scollega la periferica, l'accesso a questa viene nuovamente negato.

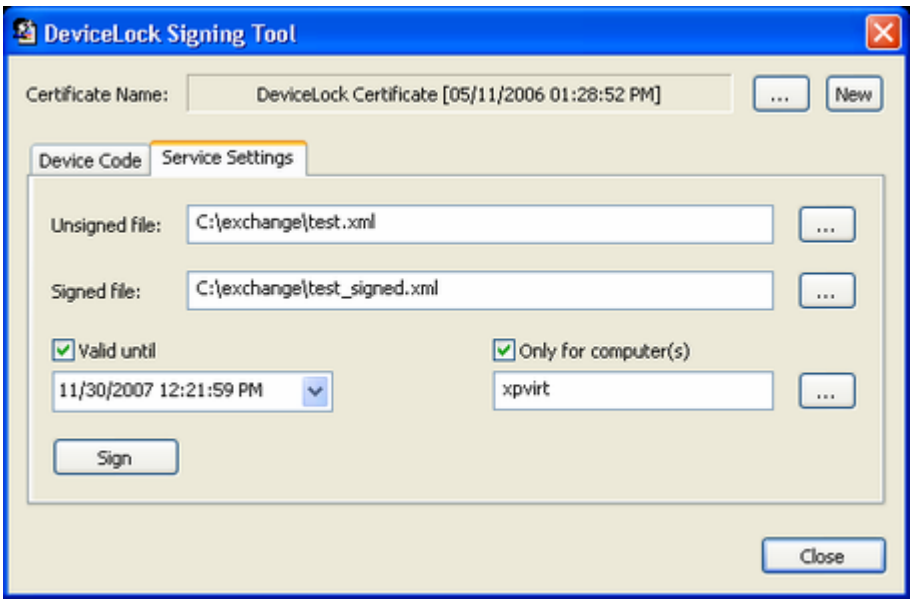
4. Fare clic sul pulsante **Generate** per creare il codice di sblocco (Unlock Code). Fornire telefonicamente o in altra maniera il codice all'utente.

   Il processo di creazione del codice di sblocco (Unlock Code) è un'operazione che richiede tempo. A seconda della velocità di elaborazione del proprio computer, l'operazione potrebbe richiedere diversi secondi per essere completata.

Impostazioni del servizio

Per impedire modifiche non autorizzate, è possibile firmare un file XML in cui sono memorizzate le impostazioni di DeviceLock Service esportate da DeviceLock Management Console o da DeviceLock Group Policy Manager o creato utilizzando DeviceLock Service Settings Editor.

Questo file potrà poi essere inviato agli utenti i cui computer non sono in linea e quindi risultano irraggiungibili dalle console di gestione.



Per firmare un file XML è sufficiente eseguire sei semplici passaggi:

1. Caricare il corrispondente certificato di DeviceLock (vedere qui).

2. Caricare il file delle impostazioni di DeviceLock Service che si desidera firmare.

   Specificare nel campo **Unsigned file** il percorso completo del file. In alternativa, per selezionare il file, fare clic sul pulsante **...**.

   Per creare il file XLM contenente le impostazioni di DeviceLock Service, scegliere **Save Service Settings** dal menu contestuale di DeviceLock Management Console, DeviceLock Group Policy Manager o DeviceLock Service Settings Editor.

3. Specificare nel campo **Signed file** il file di destinazione firmato. Per selezionare la cartella in cui salvare il file, fare clic sul pulsante **...**.
4. Scegliere se il file risultante deve contenere informazioni sulla scadenza o meno.

   Per consentire agli utenti di importare le informazioni memorizzate in questo file senza alcun limite di tempo, deselezionare la casella di controllo **Valid until**.

   Se si seleziona la casella di controllo **Valid until** e si specifica una data, le informazioni sulla scadenza verranno scritte nel file risultante. Gli utenti potranno così importare le impostazioni memorizzate nel file firmato solo entro la scadenza specificata.

   Questo parametro ha validità solamente per gli utenti che importano le impostazioni di DeviceLock Service tramite l'applet DeviceLock dal Pannello di controllo di Windows. Se si carica il file XML scegliendo **Load Service Settings** dal menu contestuale di DeviceLock Management Console o di DeviceLock Group Policy Manager, le informazioni sulla scadenza (se presenti) verranno ignorate.

5. Scegliere se consentire l'utilizzo del file risultante solo su determinati computer.

   Per consentire agli utenti di importare le informazioni memorizzate in questo file su un qualsiasi computer, deselezionare la casella di controllo **Only for computer(s)**.

   Se si seleziona la casella di controllo **Only for computer(s)** e si specificano i nomi di uno o più computer, gli utenti potranno importare le impostazioni memorizzate in questo file solo sui computer specificati. Per separare i nomi dei computer, utilizzare il punto e virgola (;).

   Nota: non è possibile specificare gli indirizzi IP dei computer. È necessario specificare i nomi dei computer così come sono visualizzati nell'applet Sistema del Pannello di controllo di Windows.

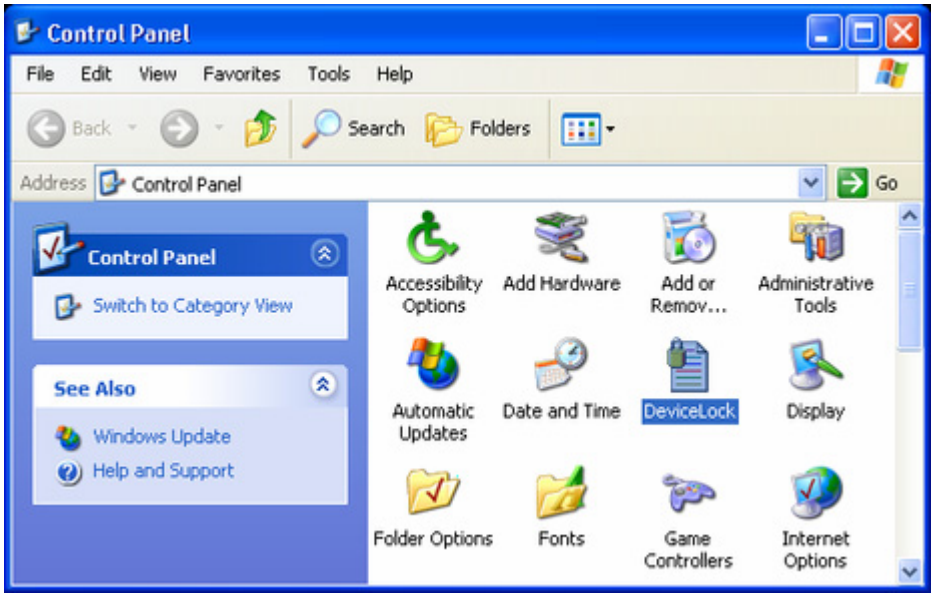
   È possibile caricare un elenco predefinito di computer da un file di testo esterno. Per caricare un file esterno, fare clic sul pulsante **...**. I nomi dei computer elencati nel file di testo devono essere specificati su righe separate.

   Questo parametro ha validità solamente per gli utenti che importano le impostazioni di DeviceLock Service tramite l'applet **DeviceLock** dal Pannello di controllo di Windows. Se si carica il file XML scegliendo **Load Service Settings** dal menu contestuale di DeviceLock Management Console o di

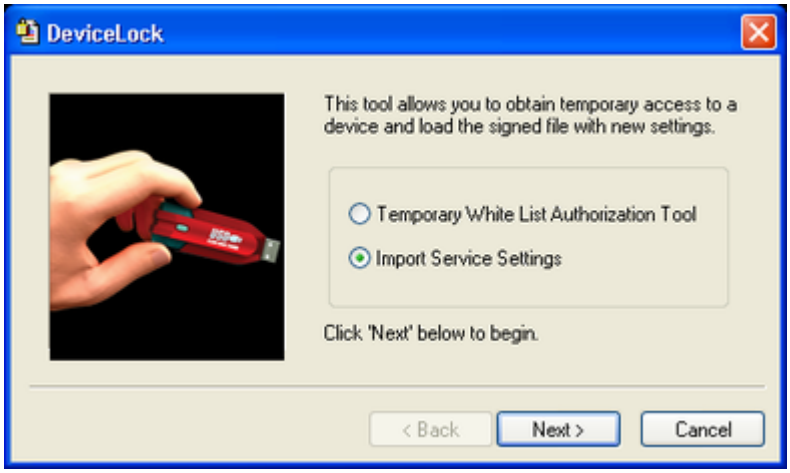
DeviceLock Group Policy Manager, le informazioni sui nomi dei computer verranno ignorate.

6. Fare clic sul pulsante **Sign** per creare un file firmato in cui sono memorizzate le impostazioni di DeviceLock Service. Distribuire quindi il file creato agli utenti. Il processo di creazione è un'operazione che richiede tempo, a seconda della velocità di elaborazione del proprio computer.

Quando un utente desidera applicare le impostazioni di DeviceLock Service importandole dal file firmato, deve avviare l'applet **DeviceLock** dal Pannello di controllo di Windows e scegliere l'opzione **Import Service Settings**.

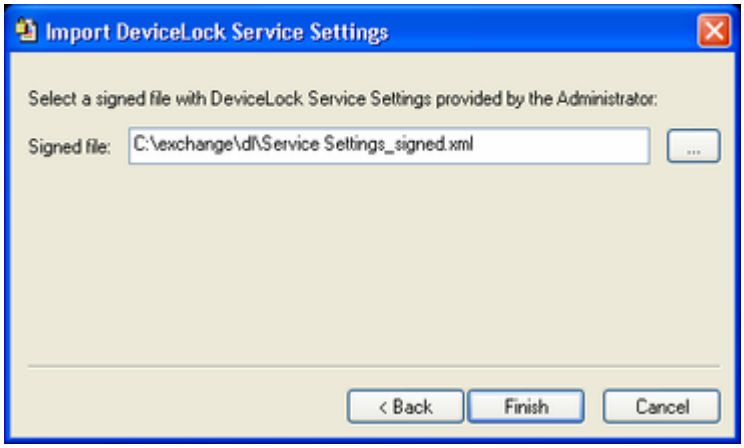


Nota: su Windows XP e versioni successive, per visualizzare tutte le applet disponibili, l'utente deve aprire il Pannello di controllo in visualizzazione classica.


DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

Per importare le impostazioni di DeviceLock Service da un file firmato, sono sufficienti due semplici passaggi:

1. Specificare nel campo **Signed file** il percorso completo del file firmato. Per selezionare il file, fare clic sul pulsante **...**.



2. Fare clic sul pulsante **Finish**. Se il file digitalmente firmato è valido, le nuove impostazioni saranno immediatamente applicate a DeviceLock Service.

L'utente inoltre può caricare il file firmato con le impostazioni DeviceLock Service mediante la riga di comando:

DLTempAccess.cpl -s *<percorso del file firmato>*

in cui *<percorso del file firmato>* è il percorso del file firmato contenente le impostazioni di DeviceLock Service. Per esempio:

DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"

Tutti i tentativi correttamente riusciti di caricare le impostazioni vengono registrati in un file di log (se la relativa opzione è stata selezionata nelle impostazioni del servizio).

DeviceLock Management Console

Informazioni generali

DeviceLock Management Console è uno snap-in per Microsoft Management Console (MMC).

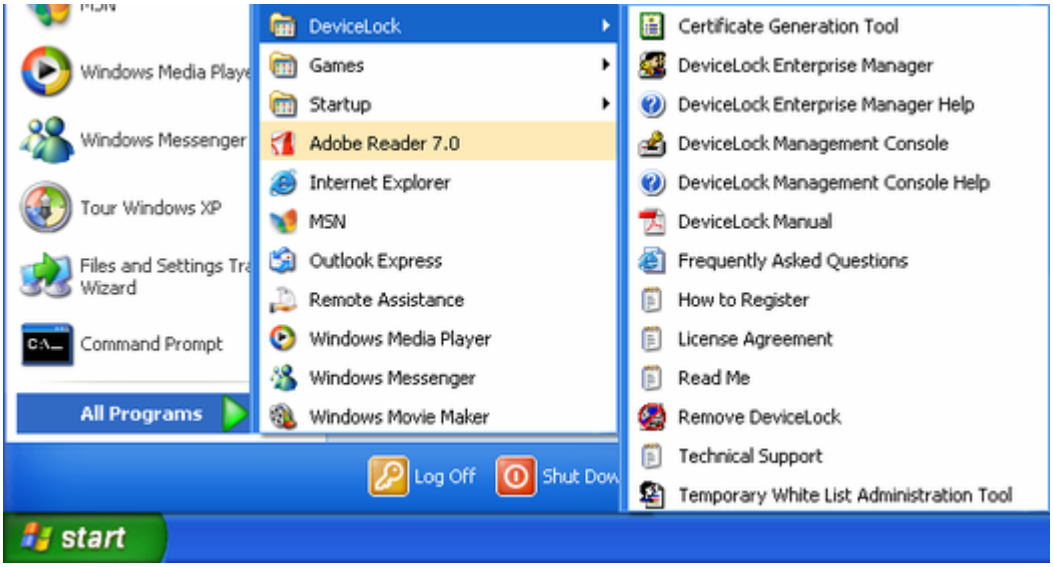
Grazie a DeviceLock Management Console, è possibile visualizzare e modificare le autorizzazioni e le regole di controllo, installare e aggiornare DeviceLock Service, visualizzare i record di controllo di ciascun computer e gestire il server su cui è in esecuzione DeviceLock Enterprise Server.

Inoltre, DeviceLock Management Console consente di visualizzare i registri degli eventi memorizzati in DeviceLock Enterprise Server, di inoltrare query di ricerca su DeviceLock Content Security Server e di gestire tali server.

DeviceLock Management Console deve essere installato sul computer utilizzato dall'amministratore per gestire in rete i servizi di DeviceLock, i DeviceLock Enterprise Server e i DeviceLock Content Security Server.

Per informazioni sull'installazione di DeviceLock Management Console, leggere la sezione Installazione delle console di gestione.

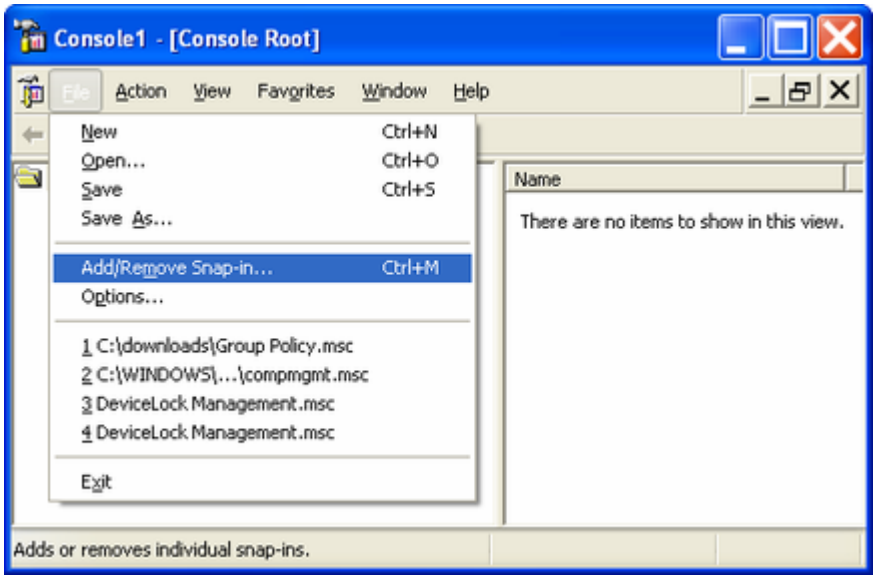
Per avviare DeviceLock Management Console, fare clic sul pulsante **Start**, quindi scegliere il collegamento dello snap-in dal menu **Tutti i programmi**.



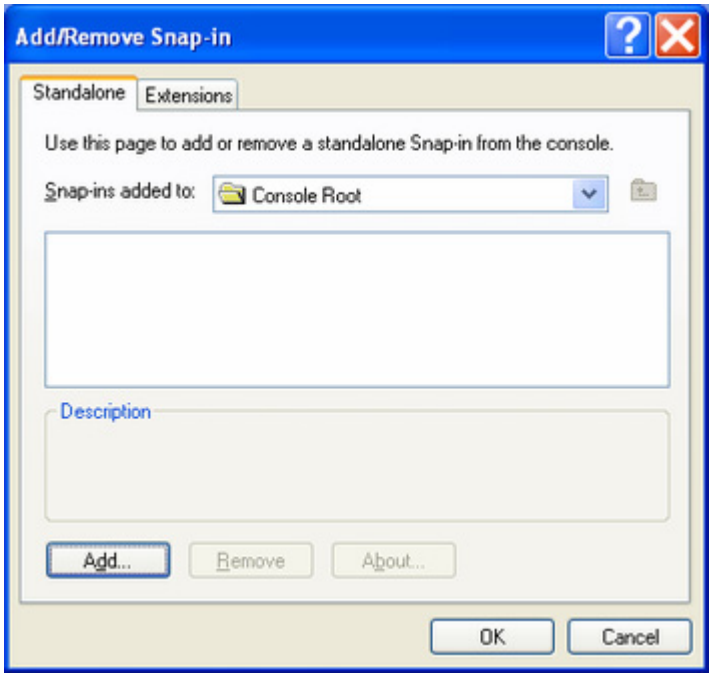
In alternativa, avviare MMC e aggiungere manualmente lo snap-in DeviceLock Management Console:

1. Avviare **mmc** dalla riga di comando oppure dalla finestra di dialogo **Esegui**.

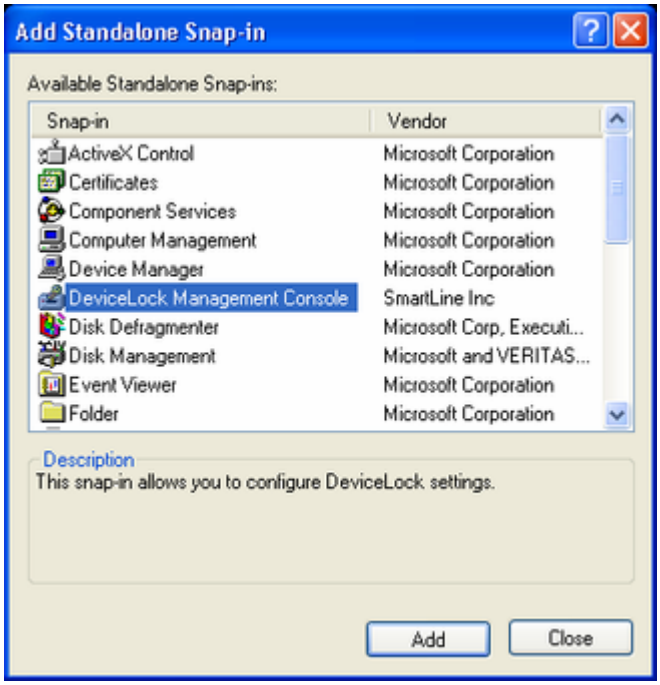
2. Aprire il menu **File** e scegliere **Aggiungi/Rimuovi snap-in**.



3. Fare clic sulla scheda **Autonomo** e quindi fare clic sul pulsante **Aggiungi**.

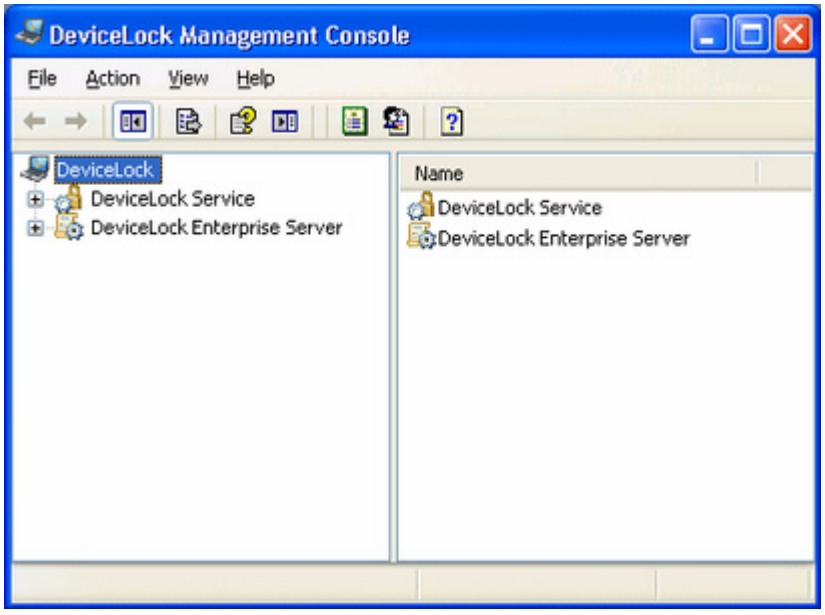


4. Selezionare **DeviceLock Management Console** dall'elenco e scegliere **Aggiungi**.



Cenni preliminari sull'interfaccia utente

L'interfaccia di DeviceLock Management Console è semplice da utilizzare ed è basata sulla tecnologia MMC (Microsoft Management Console). È possibile richiamare la Guida in linea in qualsiasi momento premendo F1.



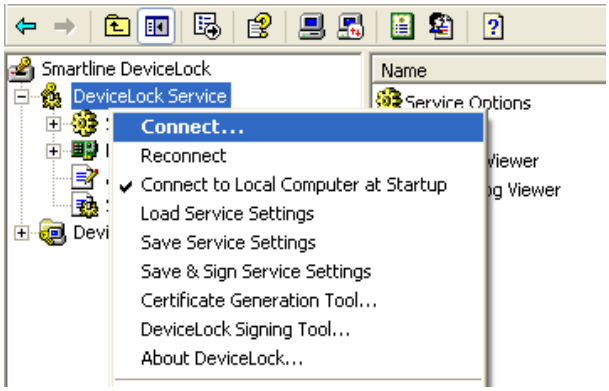
La finestra DeviceLock Management Console è composta da due riquadri. Il riquadro sinistro contiene la struttura della console, mentre quello destro i dettagli. Dopo aver selezionato un elemento nella struttura della console, le informazioni su tale elemento vengono visualizzate nel riquadro dei dettagli.

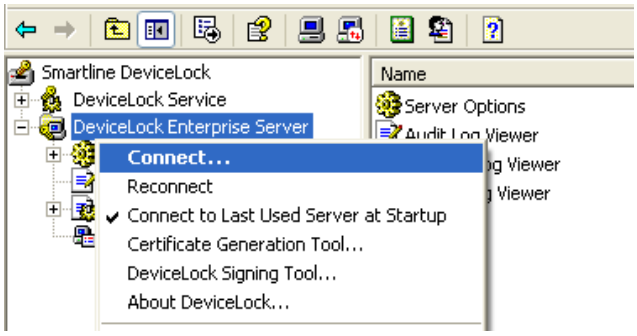
DeviceLock Management Console è costituito da tre parti indipendenti:

1. **DeviceLock Service** – consente di accedere e gestire i servizi di DeviceLock in esecuzione sui computer locali e remoti.
2. **DeviceLock Enterprise Server** – consente di accedere e gestire DeviceLock Enterprise Server in esecuzione sui computer locali e remoti.
3. **DeviceLock Content Security Server** – consente di accedere e gestire i DeviceLock Content Security Server in esecuzione sui computer locali e remoti.

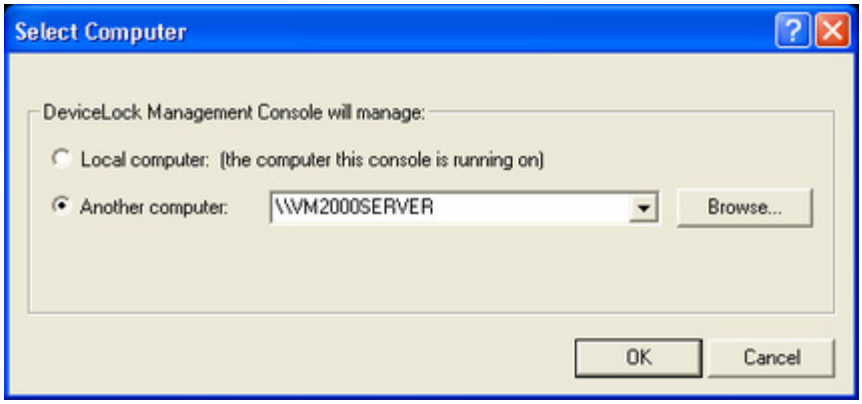
Connessione ai computer

Innanzitutto, è necessario accedere al computer su cui è in esecuzione DeviceLock Service, DeviceLock Enterprise Server o DeviceLock Content Security Server. Per connettersi al computer, scegliere **Connect** dal menu sensibile al contesto oppure fare clic sul relativo pulsante sulla barra degli strumenti.





È possibile connettersi contemporaneamente a DeviceLock Service, a DeviceLock Enterprise Server e a DeviceLock Content Security Server, anche qualora siano in esecuzione su computer differenti.



Specificare nel campo **Another computer** il nome o l'indirizzo IP del computer remoto al quale si desidera accedere. Per visualizzare i computer disponibili in rete, fare clic sul pulsante **Browse**.

Per connettere DeviceLock Management Console ad un computer su cui DeviceLock Service, DeviceLock Enterprise Server o DeviceLock Content Security Server è configurato per utilizzare una porta fissa, è necessario specificare il numero di tale porta racchiuso fra parentesi quadre, a fianco del nome del computer (ad esempio, *\\nome_computer[numero porta]*).

Per connettersi al computer locale, scegliere l'opzione **Local computer**.

Fare clic sul pulsante **OK** per effettuare la connessione al computer selezionato.

Nota: assicurarsi che il computer remoto scelto sia accessibile dal computer su cui è in esecuzione DeviceLock Management Console. Il computer remoto deve utilizzare un sistema operativo compatibile con DeviceLock (Windows NT 4.0 SP6 e versioni successive). Inoltre, è necessario che su tale computer il protocollo TCP/IP sia correttamente installato e configurato. Se sul computer remoto è installato un firewall (incluso Windows Firewall), questo deve essere correttamente configurato per consentire la connessione con DeviceLock Service, DeviceLock Enterprise Server e/o DeviceLock Content Security Server.

DeviceLock Service viene aggiunto automaticamente nell'elenco delle eccezioni di Windows Firewall.

Quando si tenta la connessione ad un computer su cui non risulta installato o aggiornato DeviceLock Service, DeviceLock Management Console richiederà l'installazione o l'aggiornamento del servizio. Per ulteriori informazioni sulla distribuzione del servizio in remoto, leggere la sezione Installazione remota tramite DeviceLock Management Console.

Quando si tenta la connessione ad un computer su cui DeviceLock Service è configurato per lavorare in modalità Criteri di gruppo, viene visualizzato un messaggio di avvertimento.

Warning
This machine is configured to use Group Policy settings. You can switch it to the Local Policy mode. In this case Group Policy settings will be replaced by Local Policy settings.
OK

Se si modificano alcuni parametri con DeviceLock Management Console, questo sarà ripristinato allo stato originale (definito in GPO) al successivo aggiornamento dei Criteri di gruppo. Per ulteriori informazioni, leggere la sezione Impostazioni del servizio.

Quando si tenta la connessione ad un computer su cui DeviceLock Enterprise Server o DeviceLock Content Security Server non risulta installato oppure è stato arrestato, viene visualizzato un messaggio di errore.

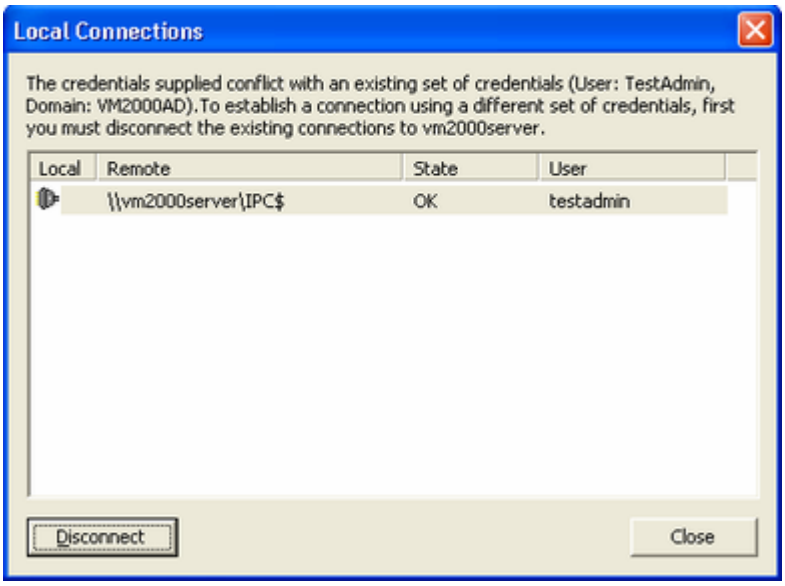
Affinché DeviceLock Management Console possa connettersi a DeviceLock Enterprise Server e DeviceLock Content Security Server, questi devono risultare installati e avviati. Per ulteriori informazioni sulla distribuzione dei server, leggere le sezioni Installazione di DeviceLock Enterprise Server e Installazione di DeviceLock Content Security Server del presente manuale.

Se non si dispone di privilegi amministrativi sul computer selezionato, DeviceLock Management Console chiederà di effettuare la connessione con un account utente differente.

Specificare nel campo **Connect As** un account utente con privilegi amministrativi. L'account utente specificato dovrebbe essere presente anche nell'elenco degli amministratori di DeviceLock qualora la funzionalità di protezione di questo amministratore sia stata attivata per DeviceLock Service, per DeviceLock Enterprise Server o per DeviceLock Content Security Server.

Un "conflitto di credenziali" si può verificare se, dopo aver effettuato il collegamento a un computer con le credenziali di un utente che non può accedere a DeviceLock Service, a DeviceLock Enterprise Server o a DeviceLock Content Security Server (ad esempio se si dispone di un disco di rete mappato, una risorsa di condivisa aperta, ecc), l'utente tenta di accedere con altre credenziali a DeviceLock Management Console. Per evitare tale conflitto, occorre prima eliminare la connessione esistente.

Quando DeviceLock Management Console rileva un conflitto di credenziali, mostra una finestra di dialogo in cui sono elencate le connessioni correntemente attive sul computer locale e richiede di eliminarne alcune.



Evidenziare tutte le connessioni attive riferite al computer desiderato e quindi fare clic sul pulsante **Disconnect**.

Infine, fare clic sul pulsante **Close** e provare nuovamente la connessione al computer.

Nota: a volte, per impedire la connessione con un account utente differente a DeviceLock Management Contole, non è possibile chiudere la connessione esistente. In questo caso, è necessario avviare DeviceLock Management Console con un account utente che disponga di privilegi sufficienti per accedere a DeviceLock Service, a DeviceLock Enterprise Server o a DeviceLock Content Security Server oppure che non abbia effettuato connessioni al computer selezionato. Per avviare DeviceLock Management Console con le credenziali di un utente differente, utilizzare la funzione "Esegui come" (digitare RUNAS sulla riga di comando) disponibile in Windows 2000 e versioni successive.

Possibili errori di connessione

Quando si tenta la connessione ad un computer su cui è in esecuzione DeviceLock Service, DeviceLock Enterprise Server o DeviceLock Content Security Server, è possibile che si verifichi uno dei seguenti errori:

- **(1722) The RPC server is unavailable** – si sta tentando la connessione ad un computer che non esiste (il nome o l'indirizzo IP non sono corretti) oppure che non è accessibile. Assicurarsi che il nome del computer specificato sia corretto. Provare ad eseguire il comando ping, specificando come parametro il nome o l'indirizzo IP del computer, e connettersi utilizzando gli strumenti

amministrativi standard di Windows (quali Gestione computer, Servizi e così via). Assicurarsi che sul computer selezionato sia installato un sistema operativo compatibile con DeviceLock (Windows NT 4.0 e versioni successive).

Inoltre, è possibile che un firewall stia bloccando l'accesso al computer. In tal caso, configurare il firewall per aprire le porte necessarie a DeviceLock. Per semplificare la configurazione del firewall, è possibile impostare DeviceLock in modo che utilizzi una porta TCP fissa. In seguito, per impostazione predefinita, DeviceLock Service, DeviceLock Enterprise Server e DeviceLock Content Security Server utilizzano le porte 9132, 9133 e 9134. Per ulteriori informazioni, leggere la sezione Domande frequenti sul nostro sito Web. Si noti che DeviceLock Service viene aggiunto automaticamente nell'elenco delle eccezioni di Windows Firewall.

- **(1753) There are no more endpoints available from the endpoint mapper** – si sta tentando la connessione a un computer su cui non è possibile accedere a DeviceLock Service, a DeviceLock Enterprise Server o a DeviceLock Content Security Server. Innanzitutto, assicurarsi che DeviceLock Service, DeviceLock Enterprise Server o DeviceLock Content Security Server siano installati e avviati sul computer remoto.

  È possibile che il computer sia stato appena avviato e che Windows stia ancora inizializzando i servizi. Il servizio Remote Procedure Call (RPC) potrebbe non essere ancora attivo.

  Inoltre, è possibile che un firewall stia impedendo l'accesso a DeviceLock Service, a DeviceLock Enterprise Server o a DeviceLock Content Security Server. Per ulteriori informazioni, leggere la descrizione dell'errore 1722.

  Per la risoluzione degli errori relativi al mapping degli endpoint RPC, leggere il seguente articolo di Microsoft: http://support.microsoft.com/kb/839880/it.

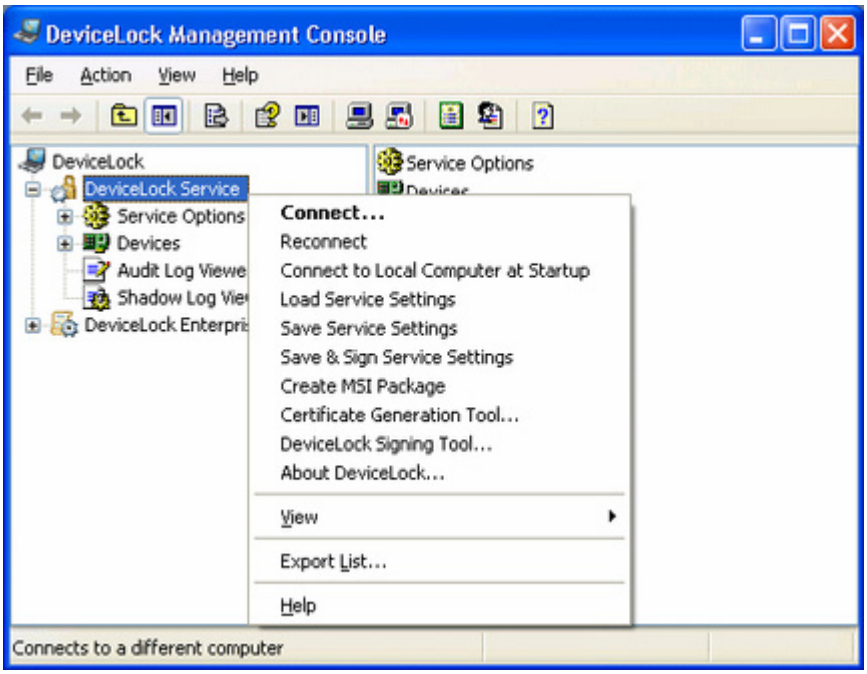
- **(5) Access is denied** – non si dispone di privilegi sufficienti sul computer remoto. Assicurarsi che DeviceLock Management Console stia tentando la connessione al computer remoto con un account utente che disponga di privilegi amministrativi locali su quel computer.

  Inoltre, è possibile che sia necessario avviare DeviceLock Management Console con un account utente differente che sia in grado di autenticarsi sul computer remoto con i privilegi amministrativi locali.

- **(7045) You must have administrative privileges to perform this operation** – non si dispone di privilegi sufficienti per accedere a DeviceLock Service, a DeviceLock Enterprise Server o a DeviceLock Content Security Server poiché l'account utente non è incluso nell'elenco degli amministratori di DeviceLock. Assicurarsi che DeviceLock Management Console stia tentando la connessione al computer remoto con un account utente incluso nell'elenco degli amministratori di DeviceLock su quel computer.

Gestione di DeviceLock Service

Espandere la voce **DeviceLock Service** per accedere alle funzioni e ai parametri di configurazione del servizio.



Fare clic con il pulsante destro del mouse per visualizzare il menu sensibile al contesto di **DeviceLock Service**:

- **Connect** – effettua la connessione al computer specificato. Per ulteriori informazioni, leggere la sezione Connessione ai computer.
- **Reconnect** – effettua nuovamente la connessione al computer al quale si è già connessi.
- **Connect to Local Computer at Startup** – DeviceLock Management Console si connette automaticamente al computer locale ad ogni avvio.
- **Load Service Settings** – carica da un file XML le impostazioni precedentemente salvate e le applica al servizio di DeviceLock correntemente connesso. È necessario selezionare un file che sia stato creato con DeviceLock Service Settings Editor, DeviceLock Management Console o DeviceLock Group Policy Manager. Poiché la firma digitale non viene convalidata in questo passaggio, il file può essere sia firmato, sia non firmato.
- **Save Service Settings** – esporta in un file XML esterno le impostazioni del servizio di DeviceLock correntemente connesso. In seguito il file può essere modificato utilizzando DeviceLock Service Settings Editor e caricato mediante DeviceLock Management Console e/o DeviceLock Group Policy Manager. Questo file può essere inviato agli utenti i cui computer non sono in linea e quindi risultano irraggiungibili dalle console di gestione. Per impedire modifiche non autorizzate al file, il file andrebbe firmato digitalmente con il

certificato di DeviceLock (chiave privata) utilizzando lo strumento DeviceLock Signing.

- **Save & Sign Service Settings** – esporta in un file XML esterno tutte le impostazioni del servizio di DeviceLock correntemente connesso e automaticamente firma digitalmente il file con il certificato più recente di DeviceLock (chiave privata). Questa voce del menu risulta disattivata se la chiave privata non è stata precedentemente caricata con lo strumento DeviceLock Signing.
- **Certificate Generation Tool** – avvia uno strumento speciale che consente di creare i certificati di DeviceLock. Per ulteriori informazioni, leggere la sezione Creazione dei certificati di DeviceLock.
- **Create MSI Package** – crea il pacchetto personalizzato Microsoft Software Installer (MSI) con le impostazioni provenienti dal DeviceLock Service collegato.

  Nel primo passaggio, è necessario selezionare il pacchetto MSI di origine con DeviceLock Service. È possibile utilizzare i pacchetti MSI inclusi in DeviceLock (ad esempio DeviceLock Service.msi e DeviceLock Service x64.msi).

  In seguito, è necessario specificare il nome del pacchetto MSI di destinazione che verrà generato in base al pacchetto MSI di origine (specificato nel primo passaggio) e alle impostazioni provenienti dal DeviceLock Service collegato.

  Successivamente, questo pacchetto MSI personalizzato potrà essere usato per implementare le istanze di DeviceLock Service all'interno della rete, utilizzando criteri predefiniti. Per maggiori informazioni sull'implementazione di DeviceLock Service utilizzando MSI, consultare la sezione Installazione tramite criteri di gruppo del presente manuale.

  Nota: se si utilizza un pacchetto MSI personalizzato, e DeviceLock Service è impostato in modo da distribuire DeviceLock Service mediante i Criteri di gruppo, queste impostazioni non si applicano ai computer client in presenza di una delle seguenti condizioni:

  - L'impostazione di protezione predefinita è disattivata nel DeviceLock Service eseguito da remoto.

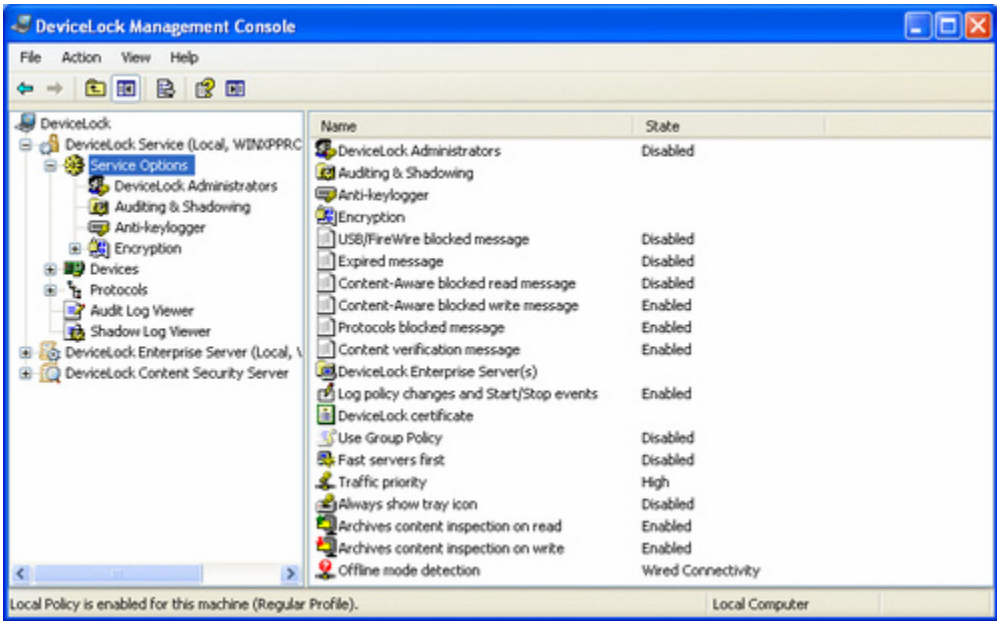
  - I Criteri di gruppo (GPO) applicati ai computer client hanno l'impostazione **Override Local Policy** attivata.

  Si noti che la voce di menu **Create MSI Package** viene disattivata se nel computer locale non è installato Microsoft Windows Installer (versione 1.0 o superiore).

- **DeviceLock Signing Tool** – avvia uno strumento speciale che consente agli utenti di accedere temporaneamente alle periferiche richieste e di firmare i file XML in cui sono incluse le impostazioni di DeviceLock Service. Per ulteriori informazioni, leggere la sezione relativa allo strumento DeviceLock Signing.
- **About DeviceLock** – mostra una finestra di dialogo e visualizza informazioni sul numero della versione di DeviceLock e sulla licenza.

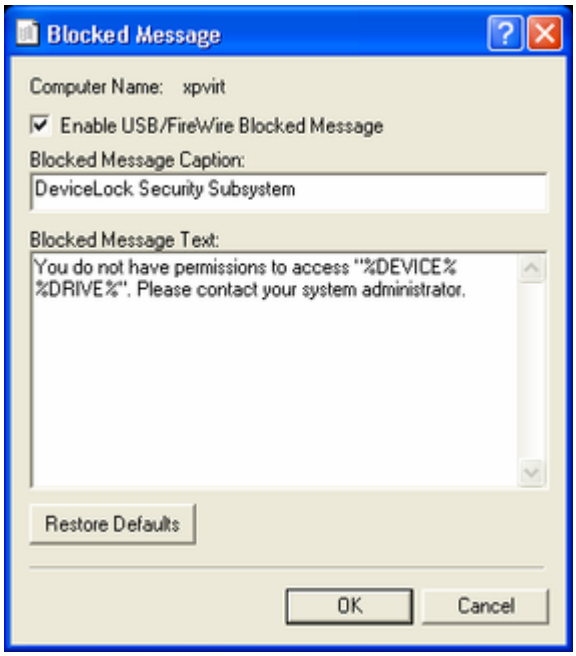
Sezione Service Options

I seguenti parametri addizionali consentono di configurare le impostazioni di DeviceLock Service. Fare clic con il pulsante destro del mouse su ciascun parametro per visualizzare il relativo menu contestuale.



Parametro “USB/FireWire blocked message”

È possibile definire un messaggio personalizzato da mostrare agli utenti in caso di accesso negato a una periferica USB o FireWire a livello di interfaccia (USB o FireWire) o di tipologia (Removable, CD/DVD, ecc.).



Per attivare la visualizzazione del messaggio personalizzato, selezionare la casella di controllo **Enable USB/FireWire Blocked Message**.

È possibile impostare parametri addizionali, quali:

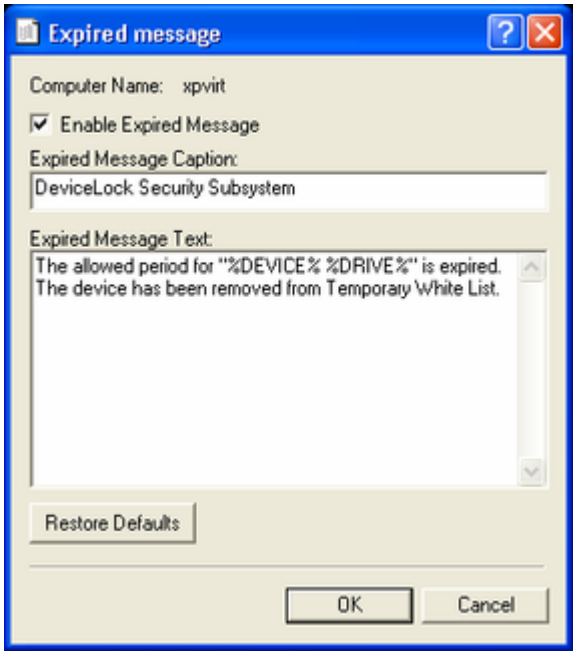
- **Blocked Message Caption** – il titolo della finestra. È possibile utilizzare tre macro predefinite:
  - **%TYPE%** – inserisce nel testo la porta a cui si sta tentando di collegare la periferica bloccata (porta USB, porta FireWire).
  - **%DEVICE%** – inserisce nel testo il nome della periferica (ad esempio, Periferica di archiviazione di massa USB) ricevuto dal sistema.
  - **%DRIVE%** – inserisce nel testo la lettera dell'unità (es. F:) assegnata alla periferica di archiviazione. Se alla periferica non è assegnata alcuna lettera, questa macro inserisce una stringa vuota.

  Grazie a queste tre macro, gli utenti possono ricevere messaggi che contengono informazioni più dettagliate.

- **Blocked Message Text** – il corpo del messaggio da visualizzare. All'interno del messaggio è possibile utilizzare le macro predefinite descritte sopra.

Parametro "Expired message"

È possibile definire un messaggio personalizzato da visualizzare all'utente quando le periferiche vengono rimosse dalla white list temporanea allo scadere del periodo di utilizzo concesso.



Per attivare la visualizzazione del messaggio personalizzato, selezionare la casella di controllo **Enable Expired Message**.

È possibile impostare parametri addizionali, quali:

- **Expired Message Caption** – il titolo della finestra. È possibile utilizzare due macro predefinite:
  - **%DEVICE%** – inserisce nel testo il nome della periferica (ad esempio, Periferica di archiviazione di massa USB) ricevuto dal sistema.
  - **%DRIVE%** – inserisce nel testo la lettera dell'unità (es. F:) assegnata alla periferica di archiviazione. Se alla periferica non è assegnata alcuna lettera, questa macro inserisce una stringa vuota.

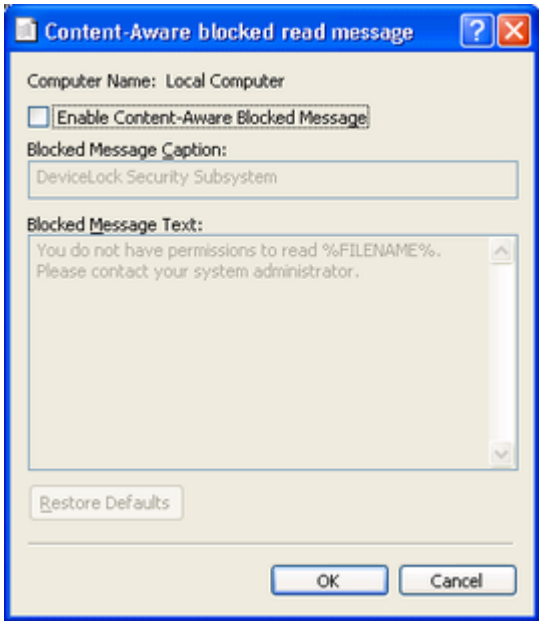
  Grazie a queste tre macro, gli utenti possono ricevere messaggi che contengono informazioni più dettagliate.

- **Expired Message Text** – il corpo del messaggio da visualizzare. All'interno del messaggio è possibile utilizzare le macro predefinite descritte sopra.

Parametro "Content-Aware Blocked Read Message"

È possibile definire la visualizzazione di un messaggio di blocco di lettura basato sul contenuto (messaggio di notifica) quando gli utenti cercano di leggere un file per cui non dispongono dell'accesso. Questo messaggio viene visualizzato nell'area di notifica della barra delle applicazioni dei computer client. Per impostazione predefinita, DeviceLock non mostra il messaggio di blocco di lettura basato sul contenuto.

Per attivare o disattivare il messaggio di blocco di lettura basato sul contenuto, fare clic con il pulsante destro del mouse su **Content-Aware blocked read message** e scegliere **Properties** o fare doppio clic su **Content-Aware blocked read message**.



Nella finestra di dialogo **Content-Aware blocked read message**, attenersi alle seguenti istruzioni:

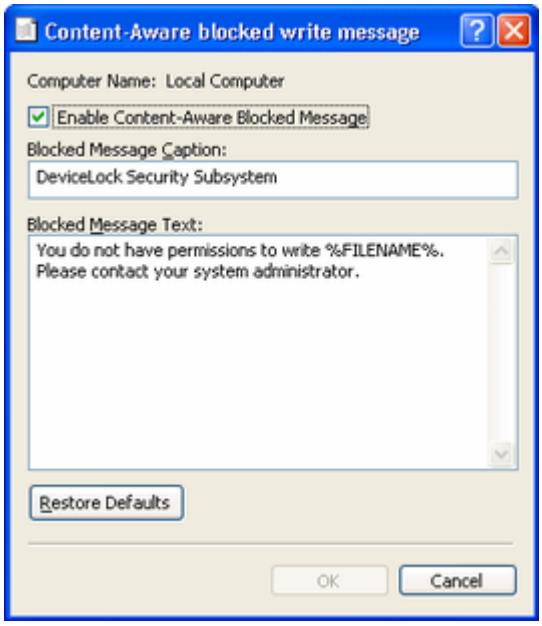
UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Enable Content-Aware Blocked Message	Attivare o disattivare il messaggio di blocco di lettura basato sul contenuto. Selezionare la casella di controllo **Enable Content-Aware Blocked Message** per attivare la visualizzazione del messaggio. Deselezionare la casella di controllo **Enable Content-Aware Blocked Message** per disattivare la visualizzazione del messaggio.
Blocked Message Caption	Specificare il testo da visualizzare nella barra del titolo della finestra del messaggio. Per impostazione predefinita, il testo di Blocked Message Caption è: **DeviceLock Security Subsystem**
Blocked Message Text	Specificare il testo da visualizzare nella finestra del messaggio. Per impostazione predefinita, il testo visualizzato nella casella Blocked Message per il messaggio di blocco di lettura basato sul contento è: **You do not have permissions to read %FILENAME%. Please contact your system administrator.** in cui **%FILENAME%** rappresenta il percorso e il nome del file da inserire.
Restore Defaults	Ripristinare le impostazioni predefinite.

Per una descrizione dettagliata della funzione Content-Aware Rules (Regole basate sul contenuto), consultare le sezioni "Regole basate sul contenuto per le periferiche (Regular Profile)" e "Regole basate sul contenuto per i protocolli (Regular Profile)".

Parametro "Content-Aware Blocked Write Message"

È possibile definire un messaggio di blocco di scrittura basato sul contenuto (messaggio di notifica) quando gli utenti cercano di scrivere su un file per cui non dispongono dell'accesso. Questo messaggio viene visualizzato nell'area di notifica della barra delle applicazioni dei computer client. Per impostazione predefinita, DeviceLock mostra il messaggio di blocco di scrittura basato sul contenuto.

Per attivare o disattivare il messaggio di blocco di scrittura basato sul contenuto, fare clic con il pulsante destro del mouse su **Content-Aware blocked write message** e scegliere **Properties** o fare doppio clic su **Content-Aware blocked write message**.



Nella finestra di dialogo **Content-Aware blocked write message**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Enable Content-Aware Blocked Message	Attivare o disattivare il messaggio di blocco di scrittura basato sul contenuto. Selezionare la casella di controllo **Enable Content-Aware Blocked Message** per attivare la visualizzazione del messaggio. Deselezionare la casella di controllo **Enable Content-Aware Blocked Message** per disattivare la visualizzazione del messaggio.
Blocked Message Caption	Specificare il testo da visualizzare nella barra del titolo della finestra del messaggio. Per impostazione predefinita, il testo di Blocked Message Caption è: **DeviceLock Security Subsystem**

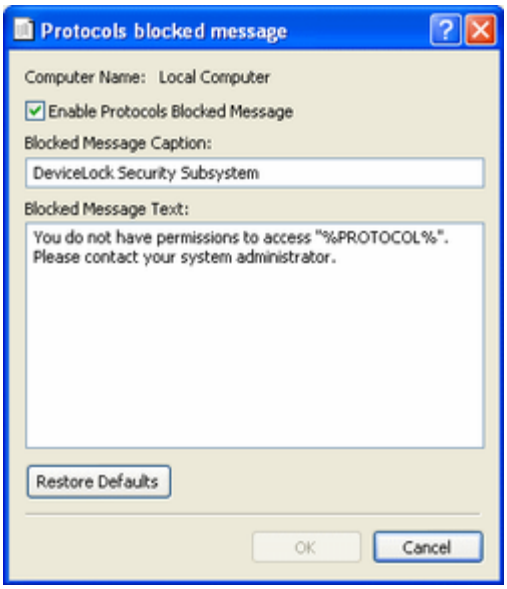
UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Blocked Message Text	Specificare il testo da visualizzare nella finestra del messaggio. Per impostazione predefinita, il testo visualizzato nella casella Blocked Message per il messaggio di blocco di scrittura basato sul contenuto è: **You do not have permissions to write %FILENAME%. Please contact your system administrator.** in cui **%FILENAME%** rappresenta il percorso e il nome del file da inserire.
Restore Defaults	Ripristinare le impostazioni predefinite.

Per una descrizione dettagliata della funzione Content-Aware Rules (Regole basate sul contenuto), consultare le sezioni "Regole basate sul contenuto per le periferiche (Regular Profile)" e "Regole basate sul contenuto per i protocolli (Regular Profile)".

Parametro "Protocols blocked message"

È possibile definire la visualizzazione di un messaggio di blocco dei protocolli (messaggio di notifica) quando gli utenti cercano di accedere a un protocollo per cui non dispongono dell'accesso. Questo messaggio viene visualizzato nell'area di notifica della barra delle applicazioni dei computer client.

Per attivare o disattivare il messaggio di blocco dei protocolli, fare clic con il pulsante destro del mouse su **Protocols blocked message** e scegliere **Properties** o fare doppio clic su **Protocols blocked message**.



Nella finestra di dialogo **Protocols blocked message**, attenersi alle seguenti istruzioni:

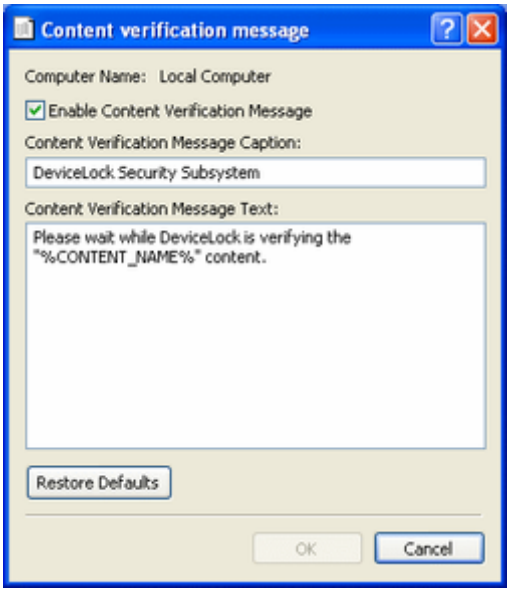
UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Enable Protocols Blocked Message	Attivare o disattivare il messaggio di blocco dei protocolli. Selezionare la casella di controllo **Enable Protocols Blocked Message** per attivare la visualizzazione del messaggio. Deselezionare la casella di controllo **Enable Protocols Blocked Message** per disattivare la visualizzazione del messaggio.
Blocked Message Caption	Specificare il testo da visualizzare nella barra del titolo della finestra del messaggio. Per impostazione predefinita, il testo di Blocked Message Caption è: **DeviceLock Security Subsystem**
Blocked Message Text	Specificare il testo da visualizzare nella finestra del messaggio. Per impostazione predefinita, il testo di Blocked Message Text è: **You do not have permissions to access %PROTOCOL%. Please contact your system administrator.** in cui **%PROTOCOL%** rappresenta il nome del protocollo da inserire.
Restore Defaults	Ripristinare le impostazioni predefinite.

Per una descrizione dettagliata della funzione Protocols (Protocolli), consultare la sezione "Protocolli (Regular Profile)".

Parametro "Content verification message"

La verifica del contenuto dei file copiati sulle periferiche o trasferiti sulla rete è un'operazione che può richiedere molto tempo. È possibile definire un messaggio di verifica del contenuto da mostrare agli utenti durante l'esecuzione dell'ispezione del contenuto. Il messaggio viene visualizzato 20 secondi dopo l'avvio della verifica del contenuto dei file da parte di DeviceLock Service.

Per attivare o disattivare il messaggio di verifica del contenuto, fare clic con il pulsante destro del mouse su **Content verification message** e scegliere **Properties** o fare doppio clic su **Content verification message**.



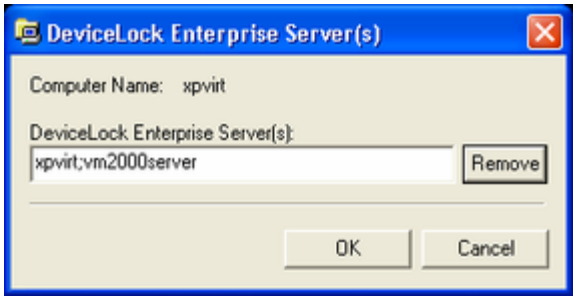
Nella finestra di dialogo **Content verification message**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Enable Content Verification Message	Attivare o disattivare il messaggio di verifica del contenuto. Selezionare la casella di controllo **Enable Content Verification Message** per attivare la visualizzazione del messaggio. Deselezionare la casella di controllo **Enable Content Verification Message** per disattivare la visualizzazione del messaggio.
Content Verification Message Caption	Specificare il testo da visualizzare nella barra del titolo della finestra del messaggio. Per impostazione predefinita, il testo di Content Verification Message Caption è: **DeviceLock Security Subsystem**
Content Verification Message Text	Specificare il testo da visualizzare nella finestra del messaggio. Per impostazione predefinita, il testo di Content Verification Message Text è: **Please wait while DeviceLock is verifying the %CONTENT_NAME% content.** in cui **%CONTENT_NAME%** rappresenta il nome del file o del protocollo da inserire. Il nome del file viene inserito mentre DeviceLock verifica il contenuto dei file copiati su una periferica. Il nome del protocollo viene inserito mentre DeviceLock verifica il contenuto dei dati trasmessi sulla rete.
Restore Defaults	Ripristinare le impostazioni predefinite.

Per una descrizione dettagliata della funzione Content-Aware Rules (Regole basate sul contenuto), consultare le sezioni "Regole basate sul contenuto per le periferiche (Regular Profile)" e "Regole basate sul contenuto per i protocolli (Regular Profile)".

Parametro "DeviceLock Enterprise Server(s)"

Per consentire a DeviceLock Service di inviare i propri registri eventi a DeviceLock Enterprise Server, è necessario specificare il nome o l'indirizzo IP del computer che ospita DeviceLock Enterprise Server.



Per bilanciare il carico della rete, è possibile specificare più server di DeviceLock Enterprise Server separati da punto e virgola (;). All'avvio, DeviceLock Service sceglie uno dei server specificati e tenta l'invio dei registri eventi. Se il server selezionato non è disponibile, DeviceLock Service sceglie un server differente.

Assicurarsi che DeviceLock Enterprise Server sia installato correttamente e sia accessibile a DeviceLock Service, altrimenti i registri eventi non verranno archiviati nel database centralizzato. Per ulteriori informazioni su come installare DeviceLock Enterprise Server, leggere la sezione Installazione di DeviceLock Enterprise Server.

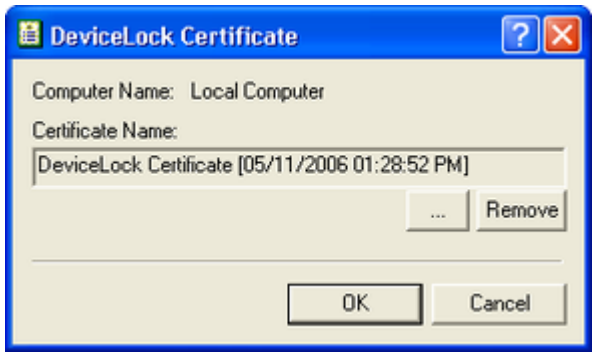
Parametro "Log Policy changes and Start/Stop event"

È possibile registrare gli eventi relativi alle modifiche apportate alla configurazione di DeviceLock Service e la registrazione degli eventi relativi all'ora di avvio e arresto di DeviceLock Service. È possibile registrare anche altri tipi di eventi, ad esempio quelli relativi alle modifiche apportate alle autorizzazioni, alle regole di controllo e alle white list.

Per attivare la registrazioni di questi eventi, selezionare l'opzione **Log Policy changes and Start/Stop events**.

Parametro “DeviceLock Certificate”

Questo parametro consente di installare o rimuovere un certificato di DeviceLock.



Per installare il certificato, specificare nel campo **Certificate Name** il percorso del file contenente la chiave pubblica. In alternativa, fare clic sul pulsante **...**. Per rimuovere la chiave pubblica, fare clic sul pulsante **Remove**.

Per ulteriori informazioni sui certificati di DeviceLock, leggere la sezione Certificati di DeviceLock.

Parametro “Use Group Policy”

Se DeviceLock Service è configurato per lavorare con i Criteri di gruppo in un dominio di Active Directory, è possibile utilizzare la modalità Group Policy oppure la modalità Local Policy.

Per attivare la modalità Group Policy, selezionare l'opzione **Use Group Policy**. In questa modalità, tutte le impostazioni configurate tramite DeviceLock Management Console e DeviceLock Enterprise Manager vengono sostituite dalle impostazioni configurate tramite Criteri di gruppo.

Per attivare la modalità Local Policy, deselezionare l'opzione **Use Group Policy**. In questa modalità, tutte le impostazioni configurate tramite DeviceLock Management Console e DeviceLock Enterprise Manager sostituiscono le impostazioni configurate tramite i Criteri di gruppo.

Se DeviceLock Service non è stato configurato per lavorare con i Criteri di gruppo, l'opzione **Use Group Policy** è disattivata e non sarà possibile selezionarla.

Se l'opzione **Use Group Policy** risulta selezionata e non è possibile deselezionarla, significa che la modalità Local Policy per questo servizio di DeviceLock non può essere attivata, poiché è stata selezionata l'opzione **Override Local Policy** in DeviceLock Group Policy Manager. Di conseguenza, le impostazioni configurate tramite DeviceLock Management Console e DeviceLock Enterprise Manager vengono sostituite dalle impostazioni configurate tramite Criteri di gruppo. Per ulteriori

informazioni, leggere la sezione Utilizzare DeviceLock Group Policy Manager.

Parametro “Fast servers first”

DeviceLock Service può scegliere il server di DeviceLock Enterprise più veloce disponibile nell'elenco dei server.

Quando questo parametro è selezionato, tutti i server specificati nel campo **DeviceLock Enterprise Server(s)** vengono suddivisi in tre gruppi, in base alla velocità della rete a cui sono collegati, e viene data precedenza al server più veloce. Se tutti i server più veloci non sono disponibili, DeviceLock Service prova a selezionare un server dal gruppo di server più veloci successivo e così via.

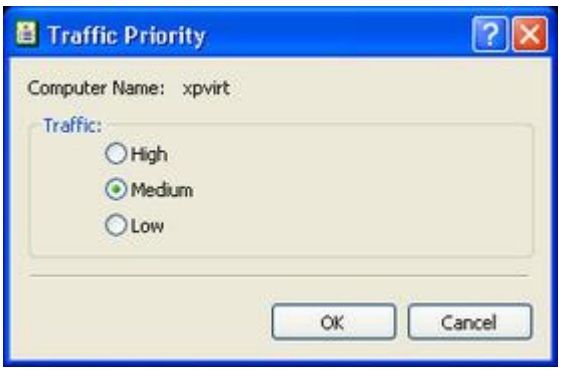
Se il parametro **Fast servers first** è disattivato, DeviceLock Service seleziona in modo casuale un server dall'elenco.

Questo parametro ha effetto solamente se nel campo **DeviceLock Enterprise Server(s)** sono specificati almeno due server.

Parametro “Traffic priority”

DeviceLock supporta lo shaping del traffico, consentendo di limitare l'ampiezza di banda utilizzata da DeviceLock Service per inviare i file di registro di controllo e di shadowing a DeviceLock Enterprise Server.

È possibile impostare tre tipi di priorità per il traffico: **High** (alto), **Medium** (medio) e **Low** (basso).



Selezionare l'opzione **High** per impostare la priorità più alta, ovvero per utilizzare l'ampiezza di banda al 100%. Selezionare l'opzione **Medium** per utilizzare fino al 50% dell'ampiezza di banda. Selezionare l'opzione **Low** per impostare la priorità più bassa, ovvero l'utilizzo dell'ampiezza di banda solo fino al 10%.

È possibile utilizzare la priorità media e bassa solamente se il componente Utilità di pianificazione pacchetti QoS di Windows è installato sul computer che esegue DeviceLock Service. In caso contrario, il parametro **Traffic priority** è disattivato e

viene utilizzata il 100% dell'ampiezza di banda. Per ulteriori informazioni su QoS, fare riferimento al seguente articolo in linea di Microsoft.

Parametro “Always show tray icon”

Utilizzare questa opzione per attivare o disattivare la visualizzazione dell'icona DeviceLock Tray Notification Utility nell'area di notifica della barra delle applicazioni dei computer client. Gli utenti finali che usano i computer client possono aggiornare lo stato di connessione (online od offline) di DeviceLock Service. Per farlo, devono fare clic con il pulsante destro del mouse sull'icona DeviceLock Tray Notification Utility nell'area di notifica della barra delle applicazioni, quindi selezionare **Refresh Current State**. Gli utenti finali, inoltre, possono fare clic sull'icona DeviceLock Tray Notification Utility per visualizzare il suggerimento di DeviceLock nell'area di notifica di un computer client.

Per attivare o disattivare la visualizzazione dell'icona DeviceLock Tray Notification Utility, fare clic con il pulsante destro del mouse su **Always show tray icon** e scegliere **Enable**/**Disable** o fare doppio clic su **Always show tray icon**.

Parametro “Archives content inspection on read”

Utilizzare questa opzione per attivare o disattivare l'ispezione dei contenuto dei file all'interno degli archivi quando gli utenti cercano di leggere questi file. Per ulteriori informazioni, leggere la descrizione della funzionalità Ispezione di file all'interno di archivi. Per attivare o disattivare l'ispezione del contenuto dei file all'interno degli archivi, fare clic con il pulsante destro del mouse su **Archives content inspection on read** e scegliere **Enable**/**Disable** o fare doppio clic su **Archives content inspection on read**.

Nota: se questa opzione viene disattivata, non viene eseguita neanche l'ispezione delle immagini incorporate nei file PDF e nei documenti RFT e Microsoft Office.

Parametro “Archives content inspection on write”

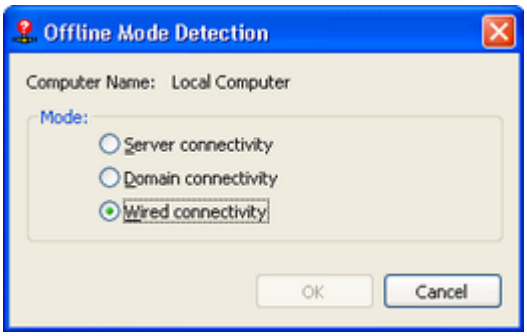
Utilizzare questa opzione per attivare o disattivare l'ispezione dei contenuto dei file all'interno degli archivi quando gli utenti cercano di scrivere su questi file. Per ulteriori informazioni, leggere la descrizione della funzionalità Ispezione di file all'interno di archivi. Per attivare o disattivare l'ispezione del contenuto dei file all'interno degli archivi, fare clic con il pulsante destro del mouse su **Archives content inspection on write** e scegliere **Enable**/**Disable** o fare doppio clic su **Archives content inspection on write**.

Nota: se questa opzione viene disattivata, non viene eseguita neanche l'ispezione delle immagini incorporate nei file PDF e nei documenti RFT e Microsoft Office.

Parametro “Offline mode detection”

Utilizzare questa opzione per configurare le impostazioni di rilevamento in modalità offline. È possibile definire le caratteristiche di rete utilizzate da DeviceLock per rilevare lo stato di connessione (online od offline). Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client.

Per configurare le impostazioni di rilevamento in modalità offline, fare clic con il pulsante destro del mouse su **Offline mode detection** e scegliere **Properties** o fare doppio clic su **Offline mode detection**.



È possibile selezionare una qualsiasi delle seguenti opzioni:

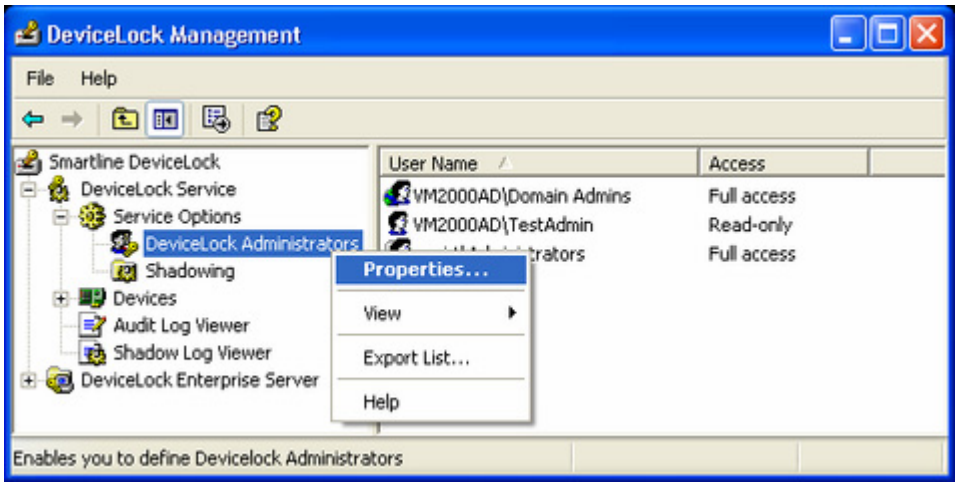
OPZIONE	DESCRIZIONE
Server connectivity	Indica che lo stato di connessione di un computer client dipende dalla possibilità di collegarsi o meno a un determinato DeviceLock Enterprise Server. Di conseguenza, un computer client opera in modalità online se può collegarsi a uno qualsiasi dei DeviceLock Enterprise Server specificati e inviare registri di controllo e shadowing ai server. Un computer client opera in modalità offline se non può collegarsi tramite autenticazione a nessuno dei DeviceLock Enterprise Server specificati o se tutti i DeviceLock Enterprise Server specificati risultano non disponibili contemporaneamente. **Procedura consigliata:** il modo più affidabile per proteggere la comunicazione client/server è l'utilizzo dell'autenticazione tramite certificato di DeviceLock. Per l'autenticazione tramite certificato client/server, la chiave pubblica deve essere installata sui computer client, mentre la chiave privata sui DeviceLock Enterprise Server. Se il certificato (la chiave pubblica) viene installato solo su DeviceLock Enterprise Server, il server respinge le connessioni e i computer client operano in modalità offline. Se il certificato (la chiave pubblica) è installato solo sui computer client, il server e il client si autenticano a vicenda quando viene stabilita una connessione. Tuttavia, questa autenticazione è meno sicura rispetto a quella basata su un certificato. Per informazioni dettagliate sui certificati di DeviceLock, consultare la sezione “Certificati di

OPZIONE	DESCRIZIONE
	DeviceLock".
Domain connectivity	Indica che lo stato di connessione di un computer client dipende dalla possibilità di collegarsi o meno al controller di dominio Active Directory appropriato (controller del dominio a cui appartiene il computer client). Di conseguenza, un computer client opera in modalità online se può collegarsi al controller di dominio appropriato. Un computer client opera in modalità offline se il controller di dominio appropriato non è disponibile. *Un computer client che non appartiene a un dominio (un computer di un gruppo di lavoro o stand-alone) opera sempre in modalità offline.*
Wired connectivity	Indica che lo stato di connessione di un computer client dipende dal collegamento o meno del cavo di rete alla scheda di interfaccia di rete (NIC). Si tratta del metodo più semplice e meno sicuro per rilevare lo stato di connessione. Di conseguenza, un computer client opera in modalità online se il cavo di rete è collegato alla scheda NIC. Un computer client opera in modalità offline se il cavo di rete non è collegato alla scheda NIC. Si noti che le connessioni di rete wireless (ad esempio Wi-Fi) e ai modem sono ignorate. Questa opzione è selezionata per impostazione predefinita.

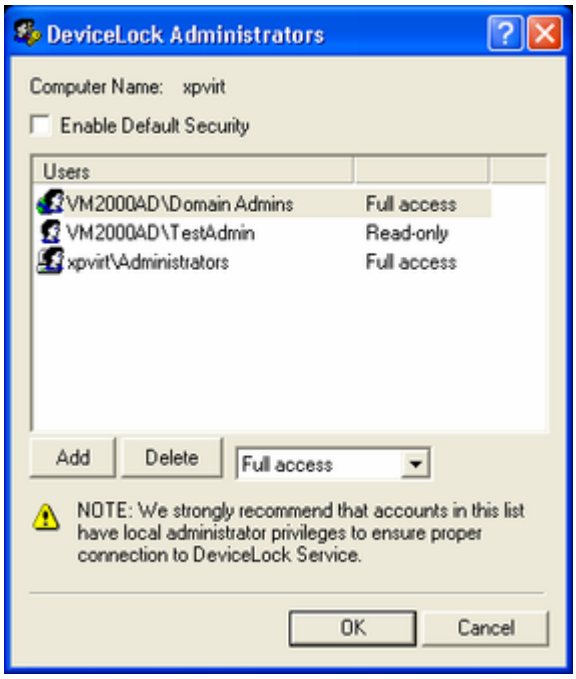
Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione di DeviceLock (Offline Profile)".

Sezione DeviceLock Administrators

Questa sezione consente di definire l'elenco degli account utenti che dispongono dei privilegi amministrativi per accedere a DeviceLock Service.



Per aprire la finestra di configurazione, fare clic con il pulsante destro del mouse sulla voce **DeviceLock Administrators** e scegliere **Properties**.



La configurazione di protezione predefinita di DeviceLock è basata sugli elenchi di controllo di accesso (Access Control Lists o ACL) di Windows. Un utente che non dispone dei privilegi di amministratore non è in grado di connettersi a DeviceLock Service, di modificarne le impostazioni o di rimuoverlo dal sistema. Ogni aspetto è controllato dal sottosistema di protezione di Windows.

Per attivare la protezione predefinita basata su ACL di Windows, selezionare l'opzione **Enable Default Security**.

Nota: come descritto nella sezione Misure di protezione di base consigliate, è fortemente sconsigliato concedere privilegi amministrativi agli utenti standard.

Gli utenti che dispongono di privilegi amministrativi locali (ovvero, i membri del gruppo locale Administrators) possono utilizzare una console di gestione per connettersi a DeviceLock Service e modificare le autorizzazioni, i controlli ed altri parametri. Questi utenti possono inoltre disinstallare DeviceLock dai propri computer, disattivare o eliminare DeviceLock Service, modificare le chiavi di Registro relative al servizio, eliminare il file eseguibile del servizio e così via. In altre parole, gli utenti che dispongono di privilegi amministrativi locali possono eludere la protezione predefinita basata su ACL di Windows.

Se, per qualche motivo, gli utenti della rete dispongono di privilegi amministrativi sui propri computer, DeviceLock fornisce un ulteriore livello di protezione: DeviceLock Security. Quando DeviceLock Security è attivo, nessun utente, ad eccezione di quelli

autorizzati, è in grado di connettersi al servizio di DeviceLock Service, di arrestarlo o di disinstallarlo. Perfino i membri del gruppo locale Administrators non possono eludere DeviceLock Security se non sono presenti nell'elenco degli amministratori autorizzati di DeviceLock.

Per attivare DeviceLock Security, deselezionare la casella di controllo **Enable Default Security**.

È necessario specificare gli account autorizzati (utenti e/o gruppi) che possono amministrare DeviceLock Service. Per aggiungere un nuovo utente o un gruppo di utenti all'elenco degli account autorizzati, fare clic sul pulsante **Add**. È possibile aggiungere più account contemporaneamente.

Per eliminare una voce dall'elenco degli account autorizzati, fare clic sul pulsante **Delete**. Per evidenziare e rimuovere più account contemporaneamente, utilizzare i tasti CTRL e/o MAIUSCOLO.

Per definire quali funzioni amministrative relative a DeviceLock assegnare ad un utente o ad un gruppo di utenti, impostare le autorizzazioni appropriate:

- **Full access** – consente l'accesso completo a DeviceLock Service. Gli utenti possono modificare le autorizzazioni, i controlli ed altri parametri, rimuovere e aggiornare DeviceLock Service.
- **Change** – consente di modificare l'accesso a DeviceLock Service. Gli utenti possono modificare le autorizzazioni, installare e rimuovere DeviceLock Service, ma non possono aggiungere nuovi utenti all'elenco degli account autorizzati ad amministrare DeviceLock Service o modificare le autorizzazioni di accesso agli utenti presenti in questo elenco.
- **Read-only** – consente solamente la lettura delle autorizzazioni, dei controlli e di altri parametri. Gli utenti possono creare report, visualizzare i parametri impostati ma non possono modificare la configurazione o rimuovere/aggiornare DeviceLock Service.

Nota: è caldamente consigliato che gli account inclusi in questo elenco dispongano di privilegi amministrativi locali poiché, in alcuni casi, l'installazione, l'aggiornamento e la disinstallazione di DeviceLock Service può richiedere i diritti di accesso al gestore controllo servizi (Service Control Manager o SCM) di Windows e alle risorse di rete condivise.

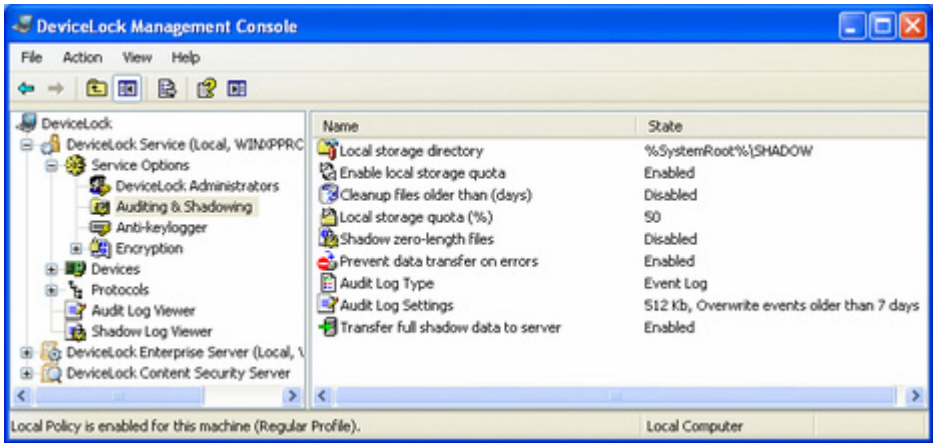
Di seguito è riportato un esempio di come definire in modo corretto l'elenco degli amministratori di DeviceLock. Aggiungere il gruppo Domain Admins, quindi assegnargli diritti di accesso completi (**Full access**). Poiché il gruppo Domain Admins è membro del gruppo locale Administrators su ciascun computer appartenente al dominio, tutti i membri del gruppo Domain Admins avranno l'accesso completo a DeviceLock Service su ogni computer. Gli altri membri del gruppo locale Administrators non saranno in grado di amministrare DeviceLock Service o di disattivarlo.

Inoltre, selezionando la casella di controllo **Enable Unhook Protection**, è possibile attivare la protezione opzionale contro le tecniche anti-rootkit che possono essere utilizzate per disattivare intenzionalmente DeviceLock Service. Se tale protezione è attivata, DeviceLock Driver verifica l'integrità del proprio codice. In presenza di violazioni, DeviceLock causa l'arresto di Windows con un errore irreversibile (BSOD).

Nota: alcuni antivirus, firewall o software di terze parti di fascia bassa possono entrare in conflitto con l'opzione Enable Unhook Protection e provocare errori irreversibili (BSOD). Si consiglia di attivare tale protezione solo sui sistemi in cui è stata precedentemente testata.

Sezione Auditing & Shadowing

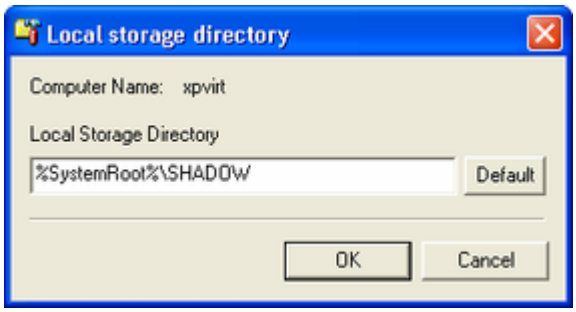
Questi parametri consentono di configurare le impostazioni per il controllo e lo shadowing di DeviceLock Service.



Utilizzare il menu sensibile al contesto richiamabile facendo clic con il pulsante destro del mouse su ciascun parametro.

Parametro "Local storage directory"

Utilizzare questo parametro per definire il punto del disco locale in cui salvare i dati della cache (per lo shadowing e l'analisi del contenuto).



Per impostazione predefinita, DeviceLock Service usa la directory ***%SystemRoot%\SHADOW*** per memorizzare i dati della cache (per lo shadowing e l'analisi del contenuto) sul computer locale. %SystemRoot% è una variabile di ambiente standard che rappresenta il percorso della cartella di installazione di Windows (ad esempio, C:\Windows). È comunque possibile specificare qualsiasi altra cartella, purché sia memorizzata su un disco accessibile localmente.

DeviceLock Service protegge la cartella specificata, in modo da impedire agli utenti regolari di accedere ai file in essa contenuti.

Assicurarsi che sul disco vi sia spazio libero sufficiente per archiviare i dati (se un utente copia 1GB di informazioni su una unità flash, sono necessari circa 2GB di spazio di archiviazione locale).

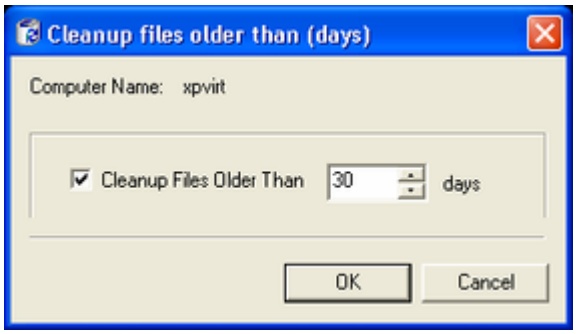
Parametro "Enable local storage quota"

Attivare questo parametro per abilitare la pulizia automatica dei dati della cache memorizzati localmente (per lo shadowing e l'analisi del contenuto).

Quando questo parametro è selezionato, è possibile configurare i parametri **Cleanup files older than (days)** e **Local storage quota (%)** (vedere sotto).

Parametro "Cleanup files older than (days) "

È possibile definire il numero di giorni trascorsi prima che i dati della cache (per lo shadowing e l'analisi del contenuto) vengano automaticamente eliminati dalla memoria locale.



Selezionare la casella di controllo **Cleanup Files Older Than** e specificare il numero di giorni che devono trascorrere prima di attivare la pulitura automatica.

Parametro "Local storage quota (%)"

È possibile definire una percentuale del disco per i dati della cache (per lo shadowing e l'analisi del contenuto).

Nel parametro **Local Storage Quota** specificare la percentuale massima (compresa tra 5 e 100) dello spazio libero sul disco rigido da utilizzare per i dati della cache.

Se la quota non viene utilizzata (ovvero, il parametro **Enable local storage quota** è disattivato), DeviceLock Service utilizza tutto lo spazio disponibile sul disco su cui è memorizzata la cartella specificata nel parametro **Local storage directory**.

Quando la dimensione totale della directory specificata nel parametro **Local storage directory** raggiunge tale percentuale, DeviceLock Service inizia a eliminare i vecchi dati se il parametro **Cleanup files older than (days)** è attivato, oppure interrompe lo shadowing dei dati e l'analisi del contenuto se il parametro **Cleanup files older than (days)** è disattivato o non vi sono dati da eliminare.

Parametro "Shadow zero-length files"

Se si attiva questo parametro, è possibile utilizzare la funzione di shadowing anche per i file con dimensione zero byte.

Anche se un file non contiene dati, è comunque possibile trasferire alcune informazioni relative al nome e al percorso (fino a parecchi kilobyte): questo è il motivo per cui potrebbe essere utile attivare lo shadowing dei file con dimensione zero byte.

Parametro "Prevent data transfer on errors"

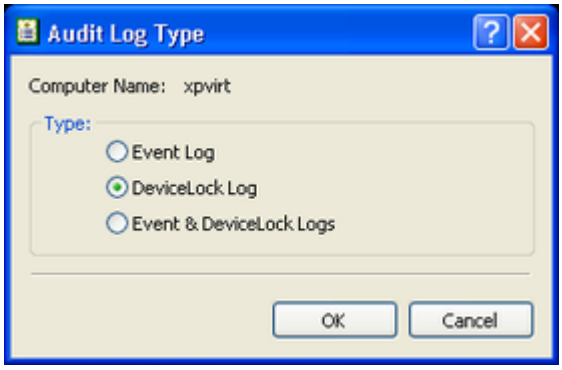
Attivando questo parametro, si impedisce agli utenti di scrivere dati se non è possibile eseguire lo shadowing o l'analisi del contenuto.

In tal modo si è sicuri del fatto che gli utenti possono trasferire informazioni solo se le regole di shadowing e basate sul contenuto funzionano normalmente (vale a dire se è presente sufficiente spazio sul disco locale per memorizzare i dati della cache).

Se il parametro **Prevent data transfer on errors** è attivato, la dimensione totale della directory specificata nel parametro **Local storage directory** raggiunge la quota specificata in **Local storage quota (%)** e non è possibile eliminare dati, DeviceLock Service interrompe lo shadowing e l'analisi del contenuto e blocca ogni tentativo di copia dei dati da parte degli utenti.

Parametro "Audit log type"

Questo parametro consente di specificare in quale registro eventi memorizzare le informazioni relative ai controlli.

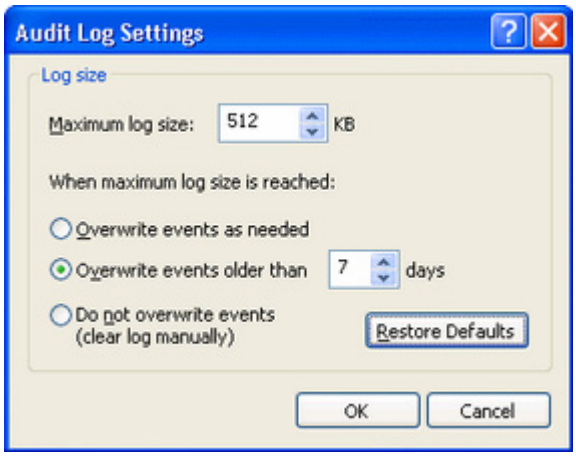


Sono disponibili tre opzioni:

- **Event Log** – le informazioni vengono memorizzate nel registro eventi locale standard di Windows.
- **DeviceLock Log** – le informazioni vengono memorizzate solamente nel registro eventi protetto di DeviceLock. I dati contenuti in questo registro vengono inviati a DeviceLock Enterprise Server e vengono archiviati centralmente nel database.
- **Event & DeviceLock Logs** – memorizza i dati in entrambi i registri eventi.

Parametro "Audit Log Settings"

Utilizzare **Audit Log Settings** per specificare la dimensione massima del registro di controllo e le opzioni di sovrascrittura.



Per una descrizione dettagliata delle impostazioni del registro di controllo, consultare la sezione "Audit Log Settings (Servizio)."

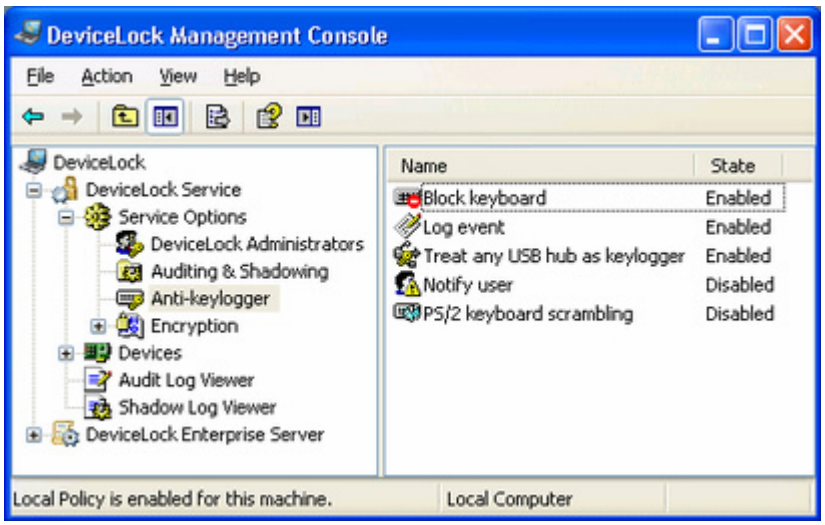
Parametro "Transfer shadow data to server"

Utilizzare questo parametro per attivare o disattivare il trasferimento di tutti i dati shadow verso DeviceLock Enterprise Server. Se il parametro **Transfer shadow data to server** è disattivato, solo i dati di controllo provenienti dal registro proprietario di DeviceLock (se il registro viene utilizzato) vengono inviati a DeviceLock Enterprise Server, mentre tutti i dati shadow vengono memorizzati localmente e non vengono trasferiti sul server.

Sezione Anti-keylogger

Questa sezione consente di configurare la modalità con cui DeviceLock Service identifica un keylogger hardware e di definire le azioni da effettuare quando ne viene identificato uno.

I keylogger hardware sono dispositivi che intercettano e registrano i tasti premuti sulla tastiera. DeviceLock Service è in grado di identificare i keylogger USB e di bloccare le tastiere ad essi collegati. DeviceLock Service, inoltre, è in grado di bloccare i keylogger PS/2.



Fare clic con il pulsante destro del mouse su ciascun parametro per visualizzarne il relativo menu contestuale.

Parametro "Block keyboard"

Se si attiva questo parametro, è possibile bloccare la tastiera connessa al keylogger hardware USB quando questo viene rilevato.

Poiché DeviceLock Service viene avviato prima della visualizzazione della finestra di accesso di Windows, questo parametro consente di bloccare la tastiera e impedire all'utente di digitare la password.

Nota: alcuni keylogger hardware continuano a registrare i tasti premuti perfino se la tastiera è bloccata e non funzionante in Windows. Questo si verifica perché alcuni keylogger sono costituiti da periferiche standalone che non richiedono alcun sistema operativo o driver per funzionare.

Parametro "Log event"

Consente di scrivere un evento nel registro eventi di controllo quando viene rilevato un keylogger hardware USB.

Parametro "Treat any USB hub as keylogger"

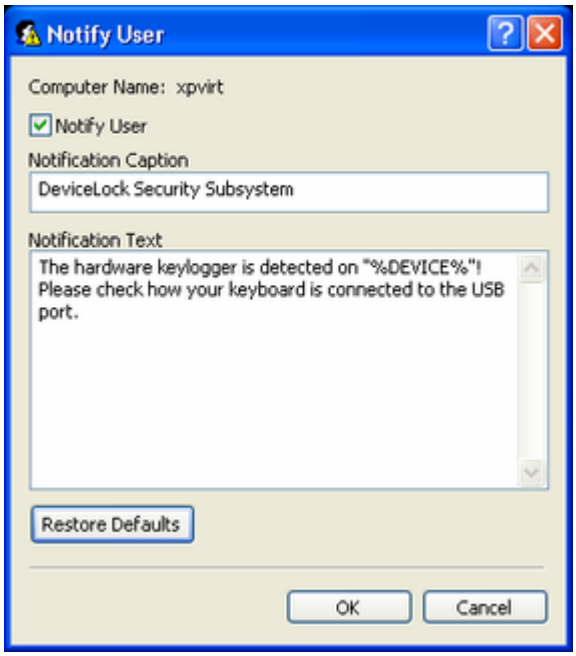
Se si attiva questo parametro, DeviceLock Service considera qualsiasi hub USB, a cui è collegata la tastiera, come un keylogger hardware.

In caso contrario, DeviceLock Service identifica solamente gli hub keylogger che sono presenti nel suo database interno.

Parametro "Notify user"

È possibile definire un messaggio personalizzato da visualizzare all'utente quando DeviceLock Service rileva un keylogger hardware USB.

Poiché DeviceLock Service viene avviato prima della visualizzazione della finestra di accesso di Windows, questo messaggio personalizzato consente di avvertire per tempo l'utente, impedendogli di digitare la password sulla tastiera collegata al keylogger USB.



Per abilitare la visualizzazione di questo messaggio, selezionare la casella di controllo **Notify User**.

È possibile definire parametri addizionali, quali i seguenti:

- **Notification Caption** – il titolo della finestra. Nel testo è possibile utilizzare delle macro predefinite: **%DEVICE%** – inserisce nel testo il nome della periferica della tastiera (es. Tastiera USB) ricevuto dal sistema.
- **Notification Text** – il corpo del messaggio da visualizzare. Nel corpo del messaggio è possibile utilizzare la macro predefinita descritta sopra.

Parametro "PS/2 keyboard scrambling"

Attivando questo parametro è possibile impedire ai keylogger PS/2 di registrare le battute. DeviceLock Service non è in grado di rilevare i keylogger PS/2 e di inviare notifiche agli utenti in merito alla loro presenza ma scherma l'input da tastiera PS/2

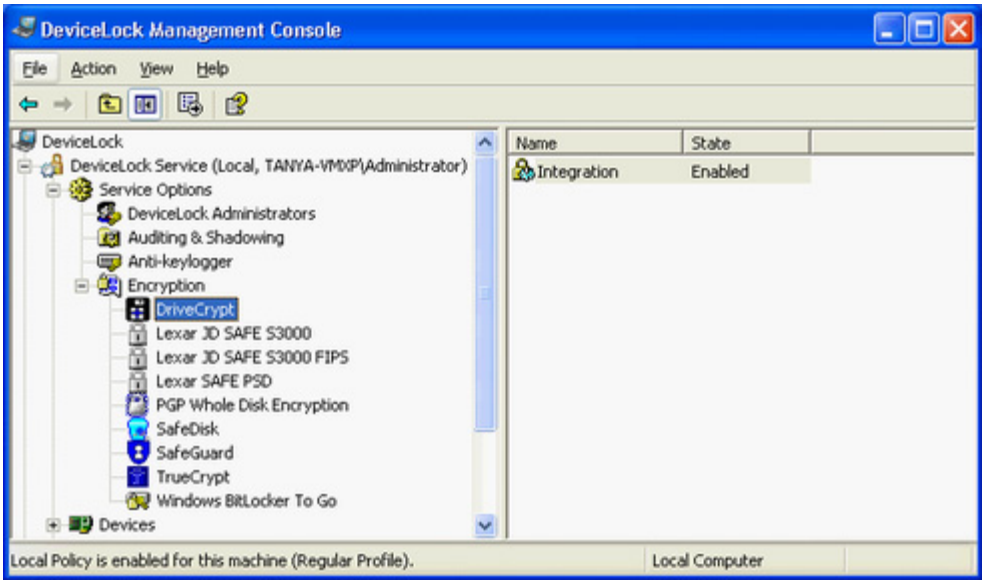
costringendo gli eventuali keylogger PS/2 a registrare sequenze di tasti prive di senso anziché le battute effettive.

Nota: se il parametro PS/2 keyboard scrambling è attivato e si utilizza lo switch PS/2 KVM, non è possibile utilizzare la tastiera per eseguire l'alternanza tra computer.

Crittografia

DeviceLock Service è in grado di rilevare i dischi (unità flash USB e altri supporti rimovibili) crittografati mediante prodotti di terzi e di applicare speciali autorizzazioni "crittografate" a tali dischi.

Questa funzionalità consente di definire criteri di controllo degli accessi più flessibili e di impedire la scrittura di dati riservati su supporti non crittografati.



Attualmente DeviceLock supporta i seguenti prodotti di terzi per la crittografia dei dati su periferiche di archiviazione rimovibili:

- **DriveCrypt** – DeviceLock Service è in grado di rilevare le periferiche di memorizzazione rimovibili crittografate con DriveCrypt e applicare autorizzazione "crittografate" speciali a tali periferiche se il prodotto DriveCrypt è installato sul computer in cui è in esecuzione DeviceLock Service e su cui è attivata l'opzione **Integration**. Per maggiori informazioni su DriveCrypt, visitare il seguente sito Web: http://www.securstar.com.
- **Lexar JD SAFE S3000** e **Lexar JD SAFE S3000 FIPS** – DeviceLock Service è in grado di rilevare le unità flash USB Lexar™ JumpDrive SAFE S3000 (certificate FIPS e/o regolari) e applicare autorizzazioni "crittografate" speciali a tali unità, nell'eventualità in cui un utente colleghi un dispositivo a un computer in cui è in esecuzione DeviceLock Service e su cui è stata attivata

l'opzione **Integration**. Per maggiori informazioni su Lexar™ JumpDrive SAFE S3000, visitare il sito Web di Lexar: http://www.lexar.com/products/enterprise-usb-solutions.

- **Lexar SAFE PSD** – DeviceLock Service è in grado di rilevare le unità flash USB Lexar™ SAFE PSD S1100 e di applicare loro autorizzazioni "crittografate" se un utente le collega a un computer su cui è in esecuzione DeviceLock Service e su cui è attivato il flag **Integration**. Per ulteriori informazioni su Lexar™ SAFE PSD S1100, visitare il sito Web di Lexar: http://www.lexar.com/about/newsroom/press-releases/lexar-begins-shipping-its-award-winning-safe-psd-s1100-secure-enterpri.
- **PGP Whole Disk Encryption** – DeviceLock Service è in grado di rilevare le periferiche di archiviazione rimovibili dotate di crittografia PGP e di applicare loro speciali autorizzazioni "crittografate" se il prodotto PGP® Whole Disk Encryption è installato sul computer in cui è in esecuzione DeviceLock Service e il flag **Integration** è attivato. Per istruzioni dettagliate su come installare e utilizzare PGP® Whole Disk Encryption con DeviceLock, fare riferimento al documento PGP/DeviceLock Integration Guide creato da PGP. Per ulteriori informazioni su PGP® Whole Disk Encryption, visitare il sito Web di PGP: http://www.pgp.com/products/wholediskencryption/index.html.
- **SafeDisk** – DeviceLock Service è in grado di rilevare i contenitori SafeDisk crittografati (memorizzati su unità flash USB e altre periferiche rimovibili) e applicare autorizzazioni speciali di crittografia se l'opzione **Integration** è attivata. Utilizzando queste autorizzazioni di crittografia, ad esempio, è possibile autorizzare la scrittura unicamente su periferiche rimovibili crittografate e impedirla su periferiche non crittografate. Per maggiori informazioni su ViPNet Safe Disk, visitare il sito Web http://www.infotecs.biz/Soft/safe_disk.htm.

  Nota: per ottenere l'accesso ai contenitori SafeDisk e utilizzarne il contenuto, gli utenti devono disporre almeno dell'accesso in lettura alle periferiche rimovibili non crittografate.

- **SafeGuard** - DeviceLock Service è in grado di rilevare i dischi crittografati tramite Sophos SafeGuard Easy (unità flash USB e altri supporti rimovibili) e di applicare agli stessi autorizzazioni speciali "crittografate" quando l'opzione **Integration** è attivata. Utilizzando queste autorizzazioni crittografate, ad esempio, è possibile autorizzare la scrittura unicamente su periferiche rimovibili crittografate e negarla su supporti non crittografati. Per maggiori informazioni su SafeGuard Easy, visitare il sito Web di Sophos Sophos Web site.
- **TrueCrypt** – DeviceLock Service è in grado di rilevare le periferiche rimovibili crittografate con TrueCrypt e di applicare loro autorizzazioni "crittografate" se il prodotto TrueCrypt viene installato in un computer su cui è in esecuzione DeviceLock Service e su cui è attivato il flag **Integration**. Per ulteriori informazioni su TrueCrypt, visitare il sito Web di TrueCrypt: http://www.truecrypt.org/.

Nota: se il tipo di volume di TrueCrypt è "**File-hosted (container)**", per accedere a tale container e lavorare con il suo contenuto, è necessario disporre almeno dell'accesso di lettura alle periferiche rimovibili non crittografate.

- **Windows BitLocker To Go** - DeviceLock Service è in grado di rilevare le unità crittografate con BitLocker To Go e di applicare autorizzazioni speciali di crittografia, a patto di attivare l'opzione **Integration**. Per ulteriori informazioni sulla funzionalità di crittografia delle unità BitLocker di Windows 7, consultare la documentazione di Microsoft pertinente.

Nota: se viene attivata l'integrazione con Windows BitLocker To Go, il criterio **Deny write access to removable drives not protected by BitLocker** (disponibile in **Configurazione computer\Modelli di Windows\Componenti di Windows\Crittografia unità BitLocker\Unità dati rimovibili**) non può essere attivato.

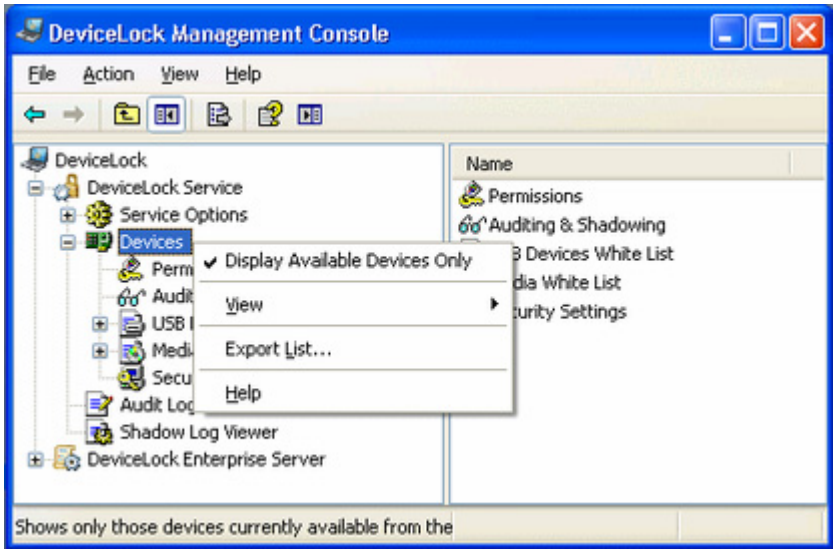
Se non si desidera che DeviceLock Service rilevi uno dei prodotti di crittografia elencati in precedenza e applichi speciali autorizzazioni "crittografate" alle periferiche di archiviazione crittografate da tale prodotto, disattivare il flag **Integration** nella sezione della console di gestione relativa al prodotto.

Per ulteriori informazioni sulle autorizzazioni "crittografate", consultare la sezione Permissions di questo manuale.

Nota: DeviceLock non è fornito unitamente a prodotti di crittografia di terzi. Tali prodotti, inoltre, non sono necessari per il funzionamento di DeviceLock. Il funzionamento integrato di DeviceLock e di un prodotto di crittografia di terzi è possibile solo se il prodotto di terzi è installato e configurato correttamente ed è in esecuzione sullo stesso computer in cui è in esecuzione DeviceLock Service.

Sezione Devices

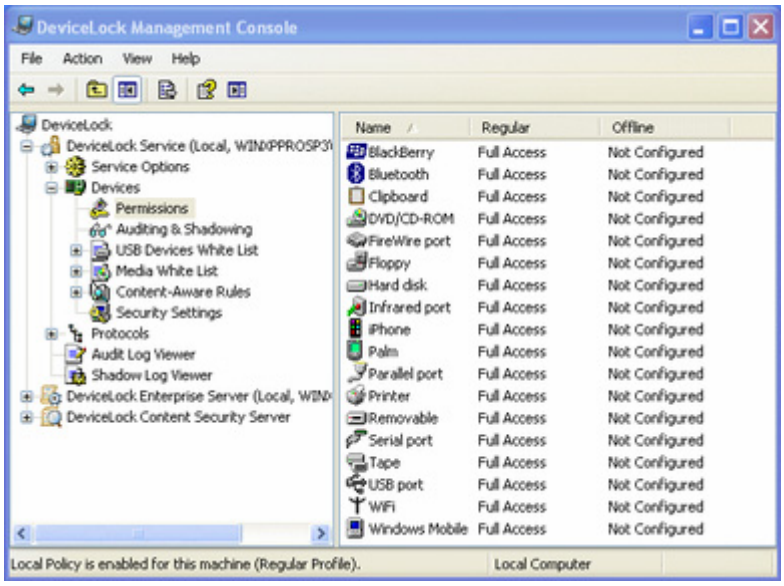
Questa sezione consente di accedere alle funzioni principali di DeviceLock, quali la definizione delle autorizzazioni, l'impostazione delle regole di controllo e di shadowing dei dati, la creazione di white list e così via.



Per accedere all'opzione **Display Available Devices Only**, fare clic on il pulsante destro del mouse sul parametro **Devices** e visualizzare il menu contestuale. Se si seleziona l'opzione **Display Available Devices Only**, DeviceLock Management Console elencherà solamente i tipi di periferica al momento disponibili sul computer corrente. Se si deseleziona l'opzione **Display Available Devices Only**, DeviceLock Management Console elencherà tutti i tipi di periferica supportati da DeviceLock. Ciò si rivela utile qualora si desideri impostare autorizzazioni di accesso per periferiche non ancora installate o momentaneamente scollegate dal computer.

Sezione Permissions (Regular Profile)

Elenca i tipi di periferiche per cui è possibile definire le autorizzazioni a livello di utente.



Nota: quando si definisce un'autorizzazione per un tipo di periferica, tale autorizzazione viene automaticamente definita per tutte le periferiche appartenenti al tipo di periferica selezionato. Non è possibile definire autorizzazioni differenti per due periferiche differenti se queste appartengono allo stesso tipo (ad esempio, due unità rimovibili). Per definire autorizzazioni differenti per periferiche USB differenti, anche se appartenenti allo stesso tipo, utilizzare la funzione White List.

Il controllo dell'accesso viene amministrato a due livelli: a livello di interfaccia (porta) e a livello di tipo. Alcune periferiche vengono controllate ad entrambi i livelli, mentre altre periferiche vengono controllate solo ad uno dei due livelli.

Per ulteriori informazioni sul controllo degli accessi, leggere la sezione Controllo dell'accesso gestito.

DeviceLock supporta i seguenti tipi di periferica:

- **BlackBerry** (livello di tipo) – include tutti i dispositivi BlackBerry con qualsiasi tipo di interfaccia di connessione (USB, Bluetooth) al computer.
- **Bluetooth** (livello di tipo) – include tutte le periferiche Bluetooth interne ed esterne dotate di qualsiasi tipo di interfaccia di collegamento al computer (USB, PCMCIA, ecc.).
- **Clipboard** - include gli Appunti di Windows. DeviceLock controlla operazioni di copia/incolla per i dati copiati negli Appunti.
- **DVD/CD-ROM** (livello di tipo) – include tutte le periferiche CD/DVD interne ed esterne (lettori e masterizzatori) dotate di qualsiasi tipo di interfaccia di collegamento (IDE, SATA, USB, FireWire, PCMCIA, ecc).
- **FireWire port** (livello di interfaccia) – include tutte le periferiche, ad eccezione degli hub, che possono essere collegate alla porta FireWire (IEEE 1394).
- **Floppy** (livello di tipo) – include tutte le unità floppy interne ed esterne dotate di qualsiasi interfaccia di collegamento (IDE, USB, PCMCIA, ecc.). È possibile che alcune unità floppy non standard siano identificate da Windows come unità rimovibili: in tal caso, DeviceLock considera tali unità floppy come tipo di periferica **Removable**.
- **Hard disk** (livello di tipo) – include tutte le unità disco fisso interne dotate di qualsiasi tipo di interfaccia di collegamento (IDE, SATA, SCSI, ecc). DeviceLock considera i dischi fissi esterni USB, FireWire e PCMCIA come tipi di periferica **Removable**. Inoltre, considera alcuni dischi fissi interni (generalmente SATA e SCSI) come tipi di periferica **Removable** se questi supportano la funzionalità hot plug e Windows non risulta installato ed in esecuzione su di essi.

  Nota: anche se si impedisce l'accesso al tipo di periferica Hard disk, gli utenti che dispongono di privilegi amministrativi locali (l'utente SYSTEM e i membri del gruppo locale Administrators) possono comunque accedere alla partizione in cui Windows è installato ed in esecuzione.

- **Infrared port** (livello di interfaccia) – include tutte le periferiche che possono essere collegate alla porta ad infrarossi (IrDA) del computer.
- **iPhone** (livello di tipo) - include tutti i tipi di periferica iPhone, iPod Touch e iPad. DeviceLock verifica le periferiche iPhone, iPod Touch e iPad collegate al PC attraverso l'applicazione iTunes o API.
- **Palm** (livello di tipo) – include tutti i dispositivi Palm OS con qualsiasi tipo di interfaccia di connessione (USB, COM, IrDA, Bluetooth, WiFi) al computer. DeviceLock controlla i dispositivi Palm OS collegati al PC tramite l'applicazione HotSync.
- **Parallel port** (livello di interfaccia) – include tutte le periferiche che possono essere collegate alla porta parallela (LPT) del computer.
- **Printer** (livello di tipo) – include tutte le stampanti locali e di rete con qualsiasi tipo di interfaccia di connessione (USB, LPT, Bluetooth, ecc.) al computer. Se lo si desidera, è possibile impostare DeviceLock per controllare

le stampanti virtuali che non inviano documenti verso periferiche reali, ma che inviano stampe su file (p. es. convertitori PDF).

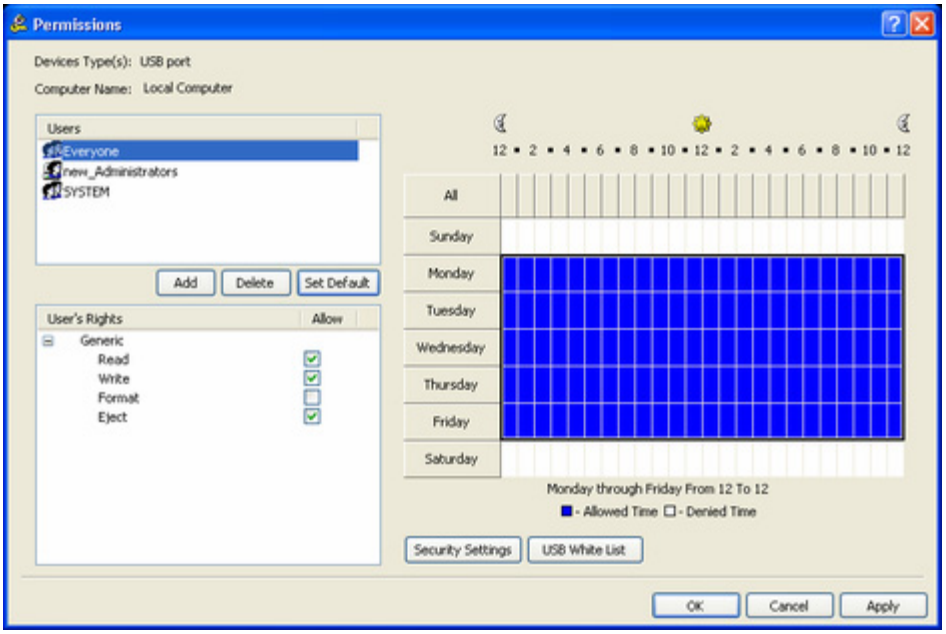
- **Removable** (livello di tipo) – include tutte le periferiche interne ed esterne dotate di qualsiasi interfaccia di collegamento (USB, FireWire, PCMCIA, IDE, SATA, SCSI, ecc) che sono identificate da Windows come unità rimovibili (ad esempio, unità flash USB, unità ZIP, lettori di card, unità magneto-ottiche e così via). DeviceLock considera i dischi fissi esterni USB, FireWire e PCMCIA come tipi di periferica **Removable**. Inoltre, considera alcuni dischi fissi interni (generalmente SATA e SCSI) come tipi di periferica **Removable** se questi supportano la funzionalità hot plug e Windows non risulta installato ed in esecuzione su di essi.
- **Serial port** (livello di interfaccia) – include tutte le periferiche che possono essere collegate alla porta seriale (COM) del computer, inclusi i modem interni.
- **Tape** (livello di tipo) – include tutte le unità a nastro interne ed esterne dotate di qualsiasi tipo di interfaccia di collegamento (SCSI, USB, IDE, ecc).
- **USB port** (livello di interfaccia) – include tutte le periferiche, ad eccezione degli hub, che possono essere collegate alla porta USB.
- **WiFi** (livello di tipo) – include tutte le periferiche WiFi interne ed esterne dotate di qualsiasi tipo di interfaccia di collegamento (USB, PCMCIA, ecc.).

  Nota: se si utilizza il tipo di periferica WiFi, è possibile controllare l'accesso effettuato dagli utenti alla periferica hardware ma non alla rete.

- **Windows Mobile** (livello di tipo) – include tutte le periferiche Windows Mobile e qualsiasi tipo di interfaccia di connessione (USB, COM, IrDA, Bluetooth, WiFi) al computer. DeviceLock controlla le periferiche Windows Mobile che funzionano assieme a un PC mediante l'applicazione Windows Mobile Device Center (WMDC) o l'applicazione Microsoft ActiveSync application o la relativa API.

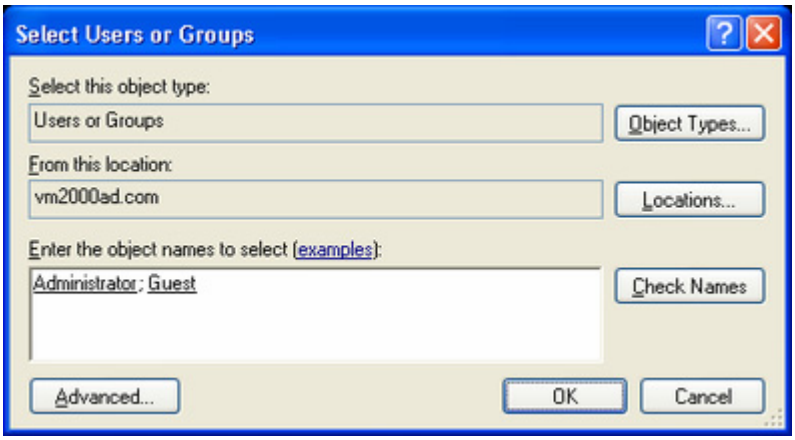
Nota: è possibile definire diverse autorizzazioni online od offline per lo stesso utente o gli stessi gruppi di utenti. Le autorizzazioni online (Regular Profile) si applicano ai computer client che operano online. Le autorizzazioni offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come impostare le autorizzazioni offline, consultare la sezione "Gestione delle autorizzazioni offline".

Per definire le autorizzazioni per un tipo di periferica, evidenziare quest'ultimo (usare i tasti Ctrl e/o Maiusc per selezionare contemporaneamente più tipi di periferica) e scegliere **Set Permissions** dal menu contestuale richiamabile con il pulsante destro del mouse. In alternativa, fare clic sul relativo pulsante sulla barra degli strumenti.



I nomi degli utenti e dei gruppi di utenti assegnati a un tipo di periferica sono visualizzati nell'elenco degli account sul lato superiore sinistro della finestra di dialogo **Permissions**.

Per aggiungere un nuovo utente o un gruppo di utenti all'elenco degli account, fare clic sul pulsante **Add**. È possibile aggiungere più account contemporaneamente.



Per eliminare una voce dall'elenco degli account, fare clic sul pulsante **Delete**. Per evidenziare e rimuovere più account contemporaneamente, utilizzare i tasti Ctrl e/o Maiusc.

Per impostare come predefinite le autorizzazioni di accesso definite per una periferica, fare clic sul pulsante **Set Default**. Le autorizzazioni predefinite vengono applicate utilizzando le seguenti selezioni di accesso:

ACCOUNT/ TIPO DI PERIFERICA	EVERYONE	ADMINISTRATORS	SYSTEM
BlackBerry	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Bluetooth	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Clipboard	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content
DVD/CD-ROM	Generic: Read, Write, Eject	Generic: Read, Write, Eject	Generic: Read, Write, Eject
FireWire port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Floppy	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Hard disk	Generic: Read, Write	Generic: Read, Write, Format	Generic: Read, Write, Format
Infrared port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
iPhone	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Palm	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Parallel port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Printer	Generic: Print	Generic: Print	Generic: Print
Removable	Generic: Read, Write, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format	Generic: Read, Write, Format, Eject Encrypted: Read, Write, Format
Serial port	Generic: Read,	Generic: Read,	Generic: Read,

ACCOUNT/ TIPO DI PERIFERICA	EVERYONE	ADMINISTRATORS	SYSTEM
	Write	Write	Write
Tape	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
USB port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
WiFi	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Windows Mobile	Generic: Read, Write, Execute	Generic: Read, Write, Execute	Generic: Read, Write, Execute

La funzione speciale Time control consente di pianificare in che ora del giorno o in quale giorno della settimana all'utente o al gruppo di utenti selezionati è concesso o meno accedere alle periferiche. La funzione Time control è visibile nella parte superiore destra della finestra di dialogo **Permissions**. Utilizzare il pulsante sinistro del mouse e selezionare il periodo di tempo in cui concedere l'accesso. Utilizzare il pulsante destro del mouse per selezionare un periodo di tempo in cui negare l'accesso. Se si utilizza la tastiera, usare i tasti di direzione per spostarsi nella griglia e utilizzare la barra spaziatrice per selezionare o deselezionare un periodo di tempo.

Per definire quali operazioni un utente o un gruppo di utenti può eseguire su una determinata periferica, impostare gli opportuni diritti. I diritti sono suddivisi in tre gruppi: **Generic**, **Encrypted** e **Special Permissions**. Ciascun gruppo possiede un insieme di diritti specifico:

- **Generic** – i diritti generici non interessano le periferiche riconosciute da DeviceLock Service come periferiche crittografate. Per ulteriori informazioni sull'integrazione della crittografia, consultare la sezione Crittografia di questo manuale.

    - **Read** – consente la lettura di dati dalla periferica. Si applica a tutti i tipi di periferica, tranne Clipboard (Appunti) e Printer (Stampante).
    - **Write** – consente la scrittura di dati sulla periferica. Fatta eccezione per Windows Mobile, è possibile attivare questo diritto per tutte le periferiche solo se **Read** è selezionato nel gruppo **Generic**. Non può essere disattivato per i tipi di periferica BlackBerry, Bluetooth, Infrared port, Parallel port, Serial port e WiFi. Se **Write** è disattivato per le porte USB e FireWire è possibile leggere dalle periferiche di archiviazione quali unità flash, unità floppy, dischi rigidi, DVD/CD-ROM, ecc. ma non scrivere sulle stesse; non è possibile accedere alle periferiche non di archiviazione quali stampanti, scanner, ecc.
    - **Format** – consente la formattazione, il controllo e ogni altro accesso diretto alle unità. È possibile attivare questo diritto solo se **Read** è selezionato nel gruppo **Generic**. Interessa esclusivamente i tipi di periferica FireWire port, Floppy, Hard disk, Removable e USB port. Se

questo diritto è attivato per le porte USB e Firewire, interessa esclusivamente le periferiche di archiviazione collegate a queste porte.

- **Eject** – consente di espellere il supporto. È possibile attivare questo diritto solo se **Read** è selezionato nel gruppo **Generic**. Questo diritto controlla esclusivamente l'espulsione tramite software. Non è possibile impedire l'espulsione dell'hardware eseguita utilizzando il pulsante di espulsione posto sul pannello anteriore di una periferica. Interessa esclusivamente i tipi di periferica DVD/CD-ROM, FireWire port, Floppy, Removable e USB port. Se questo diritto è attivato per le porte USB e Firewire, interessa esclusivamente le periferiche di archiviazione collegate a queste porte.
- **Execute** – consente l'esecuzione remota di codice sulla periferica. Interessa esclusivamente il tipo di periferica Windows Mobile.
- **Print** – consente di attivare la stampa dei documenti. Interessa esclusivamente il tipo di periferica Printer.
- **Copy to clipboard** - consente di incollare i dati provenienti dagli Appunti. Si applica unicamente al tipo di periferica Clipboard. Questo diritto garantisce automaticamente l'accesso completo agli Appunti.

- **Encrypted** – i diritti crittografati interessano esclusivamente le periferiche riconosciute da DeviceLock Service come periferiche crittografate. Per ulteriori informazioni sull'integrazione della crittografia, consultare la sezione Crittografia di questo manuale.

  - **Read** – consente la lettura di dati da una periferica crittografata. Interessa esclusivamente il tipo di periferica Removable.
  - **Write** – consente la scrittura di dati su una periferica crittografata. È possibile attivare questo diritto solo se **Read** è selezionato nel gruppo **Encrypted**. Interessa esclusivamente il tipo di periferica Removable.
  - **Format** – consente la formattazione, il controllo e ogni altro accesso diretto alle unità crittografate. È possibile attivare questo diritto solo se **Read** è selezionato nel gruppo **Encrypted**. Interessa esclusivamente il tipo di periferica Removable.

- **Special Permissions** – questi diritti si applicano solo ai tipi di periferica iPhone, Windows Mobile, Palm e Clipboard. I tipi di contenuto (Calendario, Contatti, Attività, ecc.) controllati da questi diritti per le periferiche iPhone, Windows Mobile e Palm corrispondono alle tipologie di contenuto esistenti nelle applicazioni iTunes, HotSync, Microsoft ActiveSync e WMDC. Per attivare i diritti di scrittura per i dispositivi Palm, occorre attivare i diritti di lettura corrispondenti.

  - **Read Calendar** – consente la lettura del calendario su una periferica mobile da un PC.
  - **Write Calendar** – consente la scrittura del calendario su una periferica mobile da un PC.
  - **Read Contact** – consente la lettura dei contatti su una periferica mobile da un PC.
  - **Write Contact** – consente la scrittura dei contatti da un PC su una periferica mobile.

- **Read E-mail** – consente la scrittura dei messaggi di posta elettronica da un PC su una periferica mobile. Per l'iPhone, questo tipo di contenuto rappresenta le impostazioni dell'account di posta elettronica ma non dei messaggi, in quanto iTunes non supporta la sincronizzazione dei messaggi.
- **Write E-mail** – consente la scrittura dei messaggi di posta elettronica da un PC su una periferica mobile. Per l'iPhone, questo tipo di contenuto rappresenta le impostazioni dell'account di posta elettronica ma non dei messaggi, in quanto iTunes non supporta la sincronizzazione dei messaggi.
- **Read Attachment** – consente la lettura degli allegati di posta elettronica su una periferica Windows Mobile da un PC. È possibile attivare questo diritto solo se **Read E-mail** è selezionato nel gruppo **Special Permissions**.
- **Write Attachment** – consente la scrittura degli allegati di posta elettronica da un PC su una periferica Windows Mobile. È possibile attivare questo diritto solo se **Write E-mail** è selezionato nel gruppo **Special Permissions**.
- **Read Favorite** – consente la lettura dei preferiti su una periferica Windows Mobile e iPhone da un PC.
- **Write Favorite** – consente la scrittura dei preferiti da un PC su una periferica Windows Mobile e iPhone.
- **Read File** – consente la lettura dei file da un PC su una periferica mobile. Per i dispositivi iPhone, i flussi di dati delle applicazioni di tipo iTune vengono trattati come file.
- **Write File** – consente la scrittura dei file da un PC su una periferica mobile. Su un dispositivo Palm, questo diritto attiva anche **Write Document** nel gruppo **Special Permissions**. Per i dispositivi iPhone, i flussi di dati delle applicazioni di tipo iTune vengono trattati come file.
- **Read Media** – consente la lettura di contenuti multimediali mediante Windows Media Player su una periferica Windows Mobile e la lettura di file multimediali su un dispositivo Palm da un PC. È possibile attivare questo diritto solo se **Read File** è selezionato nel gruppo **Special Permissions**. Per le periferiche Windows Mobile, è inoltre necessario selezionare **Execute** nel gruppo **Generic**. Per i dispositivi iPhone, il contenuto multimediale consiste nei seguenti tipi di iTunes: suonerie, musica, audiolibri, foto, podcast (audio e video), filmati, trasmissioni televisive, film noleggiati.
- **Write Media** – consente la scrittura di contenuti multimediali mediante Windows Media Player su una periferica Windows Mobile e la scrittura di file multimediali su un dispositivo Palm da un PC. È possibile attivare questo diritto solo se **Write File** è selezionato nel gruppo **Special Permissions**; per le periferiche Windows Mobile, è inoltre necessario selezionare **Execute** nel gruppo **Generic**. Per i dispositivi iPhone, il contenuto multimediale consiste nei seguenti tipi di iTunes: suonerie, musica, audiolibri, foto, podcast (audio e video), filmati, trasmissioni televisive, film noleggiati.
- **Read Backup** – consente di creare un backup dell'iPhone tramite la lettura dei dati del dispositivo da un PC.

Nota: iTunes effettua il backup del dispositivo iPhone ogni volta che gli utenti eseguono la sincronizzazione con iTunes (automaticamente alla prima

sincronizzazione, ogni volta che si esegue il collegamento al computer). Per eseguire correttamente la sincronizzazione, garantire l'autorizzazione **Read Backup** agli utenti del tipo di periferica **iPhone**. In caso contrario, se iTunes crea automaticamente un backup dell'iPhone, la sessione di sincronizzazione viene interrotta.

Per evitare l'interruzione della sincronizzazione, impostare iTunes in modo tale da sincronizzare solo il contenuto a cui si è autorizzati ad accedere.

- **Write Backup** – consente di ripristinare il contenuto dell'iPhone tramite la scrittura dei dati di backup del dispositivo da un PC.
- **Read Note** – consente la lettura delle note su una periferica mobile da un PC. Per i dispositivi Palm, questo diritto controlla i tipi di contenuti Memos e Note Pad.
- **Write Note** – consente la scrittura delle note da un PC su una periferica mobile. Per i dispositivi Palm, questo diritto controlla i tipi di contenuti Memos e Note Pad.
- **Read Pocket Access** – consente la lettura dei database Pocket Access su una periferica Windows Mobile da un PC.
- **Write Pocket Access** – consente la scrittura dei database Pocket Access da un PC su una periferica Windows Mobile.
- **Read Task** – consente la lettura delle attività da un PC su una periferica mobile.
- **Write Task** – consente la scrittura delle attività da un PC su una periferica mobile.
- **Read Expense** – consente la lettura dei dati applicazioni di Palm Expense su un dispositivo Palm da un PC.
- **Write Expense** – consente la scrittura dei dati applicazioni di Palm Expense da un PC su un dispositivo Palm.
- **Read Document** – consente la lettura dei documenti Palm su un dispositivo Palm da un PC. È possibile attivare questo diritto solo se **Read File** è selezionato nel gruppo **Special Permissions**.
- **Write Document** – consente la scrittura dei documenti Palm da un PC su un dispositivo Palm. È possibile attivare questo diritto solo se **Write Files** è selezionato nel gruppo **Special Permissions**.
- **Read Unidentified Content** – consente la lettura di ogni altro tipo di contenuto senza categoria su una periferica Windows Mobile da un PC.
- **Write Unidentified Content** – consente la scrittura di ogni altro tipo di contenuto senza categoria da un PC su una periferica Windows Mobile.
- **Copy Text** - consente di incollare dati testuali dagli Appunti.
- **Copy Image** - consente di incollare dati grafici dagli Appunti.
- **Copy Audio** - consente di incollare dati audio dagli Appunti.
- **Copy File** - consente di incollare file dagli Appunti.
- **Screenshot** - consente di copiare negli Appunti immagini dell'intera schermata, della finestra attiva o di qualsiasi segmento della schermata.

Nota: poiché le immagini acquisite utilizzando gli strumenti e le applicazioni di acquisizione delle schermate vengono salvate direttamente nei file, mentre le immagini acquisite premendo il tasto STAMP vengono prima copiate negli Appunti e, in seguito, incollate in un programma separato (ad esempio Microsoft Word o Paint), per controllare l'accesso alla copia delle schermate sono richiesti diversi diritti di accesso.

Per consentire agli utenti di acquisire immagini delle schermate utilizzando gli strumenti e le applicazioni pertinenti, occorre concedere loro il diritto Screenshot. Per consentire agli utenti di acquisire immagini delle schermate premendo il tasto STAMP, occorre concedere loro i diritti Screenshot e Copy Image.

Se gli utenti non possiedono il diritto Screenshot, non possono acquisire immagini delle schermate né utilizzando il tasto STAMP né utilizzando gli strumenti e le applicazioni di acquisizione delle schermate.

- **Copy Unidentified Content** - consente di incollare dagli Appunti tutti gli altri tipi di contenuto senza categoria.

Nota: i diritti Copy Text, Copy Image, Copy Audio, Copy File e Copy Unidentified Content non controllano la copia di dati negli Appunti. Gli utenti possono sempre copiare dati sugli Appunti, indipendentemente dai diritti posseduti.

Nota: se durante il processo di sincronizzazione dei dispositivi iPhone o Windows Mobile viene negato l'accesso (lettura e/o scrittura), è necessario ricollegare il dispositivo iPhone o Windows Mobile per continuare a utilizzarlo.

Se gli utenti cercano di sincronizzare un dispositivo portatile Palm all'interno di una rete e DeviceLock nega l'accesso ad alcuni tipi di contenuto, la sessione di sincronizzazione viene interrotta. Per evitare una situazione del genere, impostare l'applicazione HotSync in modo tale da sincronizzare solo il contenuto a cui si è autorizzati ad accedere prima di avviare l'operazione.

Se per un account utente sono attivati tutti i diritti, l'account dispone di diritti di "accesso completo" a una periferica. Se per un account utente sono disattivati tutti i diritti, l'account è caratterizzato da "assenza completa di diritti di accesso" a una periferica.

Nota: l'"assenza completa di diritti di accesso" ha la priorità rispetto a ogni altro diritto. Ciò significa che se il gruppo di appartenenza di un utente è caratterizzato da "assenza completa di diritti di accesso" e l'utente dispone di "accesso completo", l'utente non può comunque accedere a una determinata periferica. Se si desidera negare l'accesso a un particolare utente o gruppo, è sufficiente rimuoverlo dall'elenco degli account; non è necessario aggiungerlo con "assenza completa di diritti di accesso".

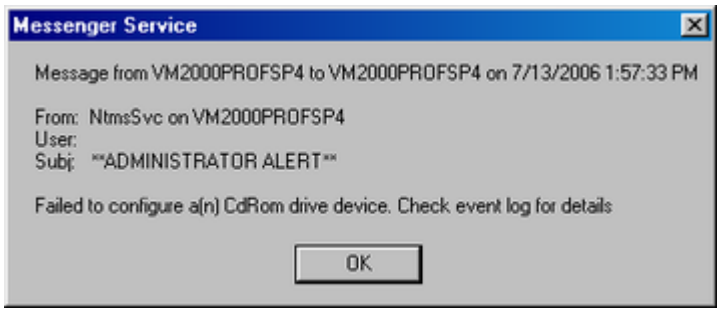
Inoltre, l'utente Everyone ha la priorità rispetto a ogni altro account. Ciò significa che se Everyone presenta "assenza completa di diritti di accesso", nessun utente è autorizzato ad accedere a una periferica.

Anche se si impedisce l'accesso al tipo di periferica Hard disk, gli utenti che dispongono di privilegi amministrativi locali (l'utente SYSTEM e i membri del gruppo locale Administrators) possono comunque accedere alla partizione in cui Windows è installato ed in esecuzione.

Si consiglia di aggiungere in elenco solamente gli account (utenti e/o gruppi) a cui è concesso accedere alla periferica. Se l'elenco degli account è completamente vuoto, nessun utente sarà in grado di accedere alla periferica.

Si consiglia inoltre di aggiungere l'utente SYSTEM con i privilegi di "accesso completo" per i tipi di periferica Hard Disk e DVD/CD-ROM.

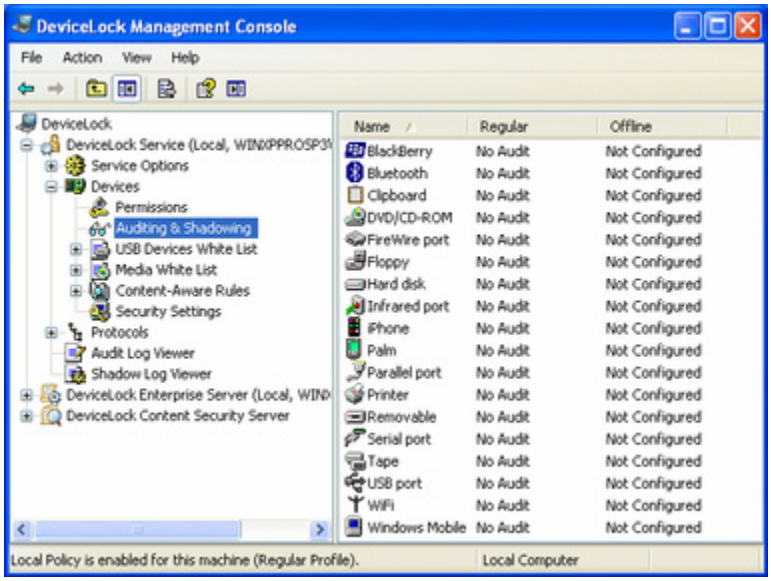
Su alcuni sistemi, gli utenti potrebbero visualizzare il seguente messaggio durante l'accesso a Windows.


Messenger Service
Message from VM2000PROFSP4 to VM2000PROFSP4 on 7/13/2006 1:57:33 PM
From: NtmsSvc on VM2000PROFSP4
User:
Subj: **ADMINISTRATOR ALERT**
Failed to configure a(n) CdRom drive device. Check event log for details
OK

Questo significa che l'utente SYSTEM non può accedere alle periferiche DVD/CD-ROM. Per evitare di visualizzare questo messaggio in futuro, assegnare all'utente SYSTEM il privilegio di "accesso completo" per i tipi di periferica DVD/CD-ROM.

Sezione Auditing & Shadowing (Regular Profile)

Elenca i tipi di periferica per cui è possibile definire le regole di controllo e di shadowing a livello di utente.



Non esistono grosse differenze tra impostare le autorizzazioni e definire le regole di controllo e di shadowing, quindi si consiglia di leggere prima la sezione Permissions.

Per registrare le informazioni relative ad una periferica, DeviceLock può utilizzare il sottosistema standard di registrazione degli eventi di Windows. Questo risulta

particolarmente utile agli amministratori di sistema, poiché possono utilizzare un qualsiasi software di visualizzazione degli eventi, quale ad esempio Visualizzatore eventi, per leggere gli eventi di controllo di DeviceLock. Inoltre, DeviceLock Service può memorizzare gli eventi di controllo utilizzando un proprio formato proprietario protetto ed inviare i dati raccolti a DeviceLock Enterprise Server per archiviarli centralmente in un database. Per definire la modalità di registrazione degli eventi, impostare in modo appropriato il parametro **Audit log type** (vedere la sezione Impostazioni del servizio).

DeviceLock Management Console dispone di un proprio visualizzatore degli eventi di controllo, in grado di visualizzare le informazioni raccolte in una forma più conveniente. Per ulteriori informazioni, leggere Sezione Audit Log Viewer (Servizio).

Per visualizzare gli eventi di controllo archiviati nel database di DeviceLock Enterprise Server, utilizzare il visualizzatore degli eventi del server.

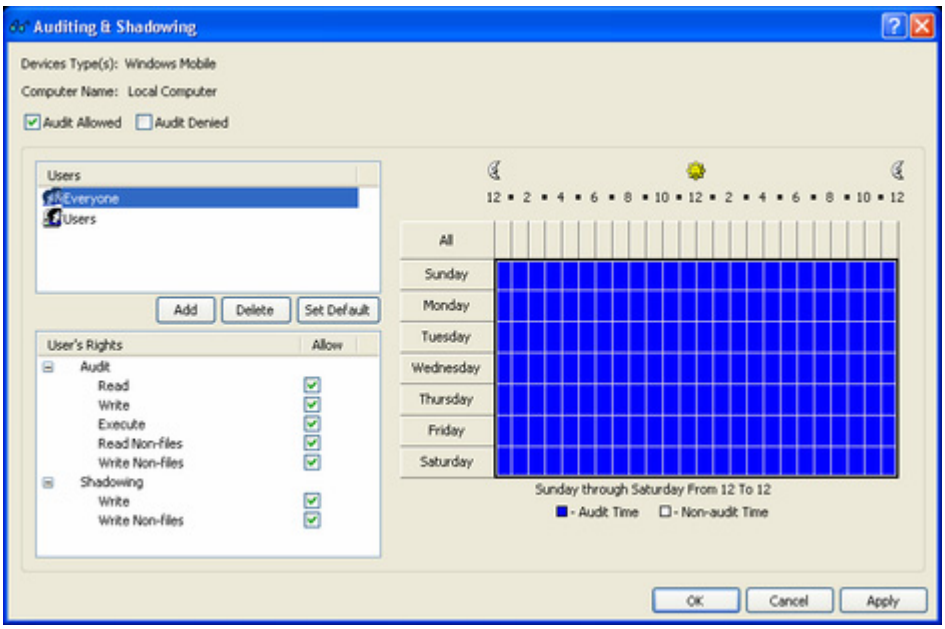
Esiste anche una funzionalità di controllo avanzata chiamata shadowing dei dati, ovvero la capacità di effettuare il mirroring di tutti i dati copiati su un supporto di archiviazione esterno o trasferiti attraverso le porte seriali e parallele. Viene effettuata la registrazione di tutti i dati copiati. Gli eventi di shadowing vengono archiviati localmente in una cartella speciale (vedere Impostazioni del servizio) e possono essere trasferiti a DeviceLock Enterprise Server e archiviati in un database SQL, in base ai parametri specificati nelle impostazioni del servizio.

Per visualizzare gli eventi di shadowing archiviati localmente, utilizzare il visualizzatore degli eventi di shadowing incorporato in DeviceLock Management Console. Per ulteriori informazioni, leggere Sezione Shadow Log Viewer (Servizio).

Per visualizzare gli eventi di shadowing archiviati nel database di DeviceLock Enterprise Server, utilizzare il visualizzatore degli eventi del server.

Nota: è possibile definire diverse regole di controllo e shadowing online od offline per lo stesso utente o gli stessi gruppi di utenti. Le regole di controllo e shadowing online (Regular Profile) si applicano ai computer client che operano online. Le regole di controllo e shadowing offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire le regole di controllo e shadowing offline, consultare la sezione "Gestione delle regole di controllo e shadowing offline".

Per definire le regole di controllo e di shadowing per un tipo di periferica, evidenziare quest'ultimo (usare i tasti Ctrl e/o Maiusc per selezionare contemporaneamente più tipi di periferica) e scegliere **Set Auditing & Shadowing** dal menu contestuale richiamabile con il pulsante destro del mouse. In alternativa, fare clic sul relativo pulsante sulla barra degli strumenti.



È possibile registrare due tipi di accesso utente:

- **Allowed** – tutti i tentativi di accesso concessi da DeviceLock Service - l'utente è stato in grado di accedere alla periferica.
- **Denied** – tutti i tentativi di accesso che sono stati bloccati da DeviceLock Service - l'utente non è stato in grado di accedere alla periferica.

Per attivare la registrazione degli eventi di controllo per uno o entrambi i tipi di accesso, selezionare **Audit Allowed** e/o **Audit Denied**. Queste opzioni non sono collegate agli utenti/gruppi, ma sono relative al tipo di periferica.

I nomi degli utenti e dei gruppi di utenti assegnati a un tipo di periferica sono visualizzati nell'elenco degli account sul lato superiore sinistro della finestra di dialogo **Auditing & Shadowing**.

Per aggiungere un nuovo utente o gruppo di utenti all'elenco degli account, fare clic sul pulsante **Add**. È possibile aggiungere più utenti contemporaneamente.

Per eliminare un elemento dall'elenco degli account, selezionarlo e quindi fare clic sul pulsante **Delete**. Per evidenziare ed eliminare più elementi contemporaneamente, utilizzare i tasti Ctrl e/o Maiusc.

Utilizzare il pulsante **Set Default** per impostare le regole di controllo e di shadowing predefinite per le periferiche: i diritti di controllo e di shadowing **Read** e **Write** dei membri del gruppo Users e dell'account Everyone sono disattivati.

La funzione speciale Time control consente di pianificare in che ora del giorno o in quale giorno della settimana attivare o meno le regole di controllo per l'utente o gruppo di utenti selezionati. La funzione Time control è visibile nella parte superiore

destra della finestra di dialogo **Auditing & Shadowing**. Utilizzare i pulsanti sinistro o destro del mouse per, rispettivamente, definire il periodo di tempo in cui attivare o disattivare la regola. Se si utilizza la tastiera, usare i tasti di direzione per spostarsi nella griglia e utilizzare la barra spaziatrice per selezionare o deselezionare un periodo di tempo.

Per definire quali operazioni eseguite da un utente o da un gruppo di utenti su una determinata periferica sono registrate nel registro di controllo o di shadowing, impostare gli opportuni diritti di controllo. I diritti sono suddivisi in due gruppi: **Audit** e **Shadowing**. Ciascun gruppo possiede un insieme di diritti specifico:

- **Audit** – i diritti appartenenti a questo gruppo determinano le azioni registrate nel registro di controllo.
    - **Read** – consente di registrare i tentativi di accesso in lettura. Per i tipi di periferica BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port e WiFi è possibile attivare questo diritto solo se **Write** è selezionato nel gruppo **Audit**.
    - **Write** – consente di registrare i tentativi di accesso in scrittura. Per i tipi di periferica BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port e WiFi è possibile attivare questo diritto solo se **Read** è selezionato nel gruppo **Audit**.
    - **Print** – consente di registrare i tentativi di invio di documenti alle stampanti. Interessa esclusivamente il tipo di periferica Printer.
    - **Execute** – consente di registrare i tentativi di accesso mirati all'esecuzione remota di codice sulla periferica. Interessa esclusivamente il tipo di periferica Windows Mobile.
    - **Read Non-files** – consente di registrare i tentativi di accesso in lettura per gli oggetti diversi dai file (Calendario, Contatti, Attività, ecc.). Interessa esclusivamente i tipi di periferica iPhone, Windows Mobile e Palm.
    - **Write Non-files** – consente di registrare i tentativi di accesso in scrittura per gli oggetti diversi dai file (Calendario, Contatti, Attività, ecc.). Interessa esclusivamente i tipi di periferica iPhone, Windows Mobile e Palm.
    - **Copy** - consente di registrare tutti i tentativi di incollare dati dagli Appunti e di acquisire schermate. Si applica unicamente agli Appunti.
- **Shadowing** – i diritti appartenenti a questo gruppo determinano le azioni registrate nel registro di shadowing.
    - **Write** – consente di eseguire lo shadowing dei dati scritti dall'utente. Interessa esclusivamente i tipi di periferica DVD/CD-ROM, Floppy, iPhone, Parallel port, Removable, Serial port, Windows Mobile e Palm.
    - **Print** – consente di eseguire lo shadowing dei documenti inviati alle stampanti. In seguito, questi documenti possono essere visualizzati utilizzando DeviceLock Printer Viewer. Interessa esclusivamente il tipo di periferica Printer.
    - **Write Non-files** – consente di eseguire lo shadowing degli oggetti diversi dai file (Calendario, Contatti, Attività, ecc.) scritti dall'utente.

Interessa esclusivamente i tipi di periferica iPhone, Windows Mobile e Palm.

La seguente tabella riporta i diritti di controllo assegnabili ai vari tipi di periferica e la natura delle informazioni scritte nel registro. Per ogni evento, DeviceLock Service memorizza il tipo di evento, la data e l'ora, il tipo di periferica, il nome dell'utente, le informazioni sul processo e le informazioni sull'evento descritte nella seguente tabella.

TIPO DI PERIFERICA	**DIRITTI**
BlackBerry	• Audit: Read + *L'azione Device Access viene scritta nel registro di controllo*. • Audit: Write/Print + *L'azione Device Access viene scritta nel registro di controllo*. • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
Bluetooth	• Audit: Read + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Write/Print + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
Clipboard	• Audit: Read — • Audit: Write/Print — • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy + *Le azioni Copy Text, Copy File, Copy Image, Copy Audio, Copy Unidentified e Screenshot vengono registrate sul registro di controllo*. • Shadowing: Write/Print — • Shadowing: Write Non-files —
DVD/CD-ROM	• Audit: Read + *Gli eventi Open, Device Access, Direct Access e Eject, nomi dei file e flag (Read, DirectRead, Eject, DirList) sono scritti nel registro di*

TIPO DI PERIFERICA	DIRITTI
	controllo. • Audit: Write/Print + *Gli eventi Open, Device Access e Direct Access e i flag (Write, Del, DirectWrite) sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *Le immagini CD/DVD in formato CUE e/o i file sono scritti nel registro di shadowing.* • Shadowing: Write Non-files —
FireWire port	• Audit: Read + *Le azioni Insert, Remove e Device Access e i nomi delle periferiche sono scritti nel registro di controllo.* • Audit: Write/Print + *Le azioni Insert, Remove e Device Access e i nomi delle periferiche sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
Floppy	• Audit: Read + *Le azioni Open, Mount, Unmount e Direct Access, nomi dei file e flag (Read, DirectRead, Eject, DirList) sono scritti nel registro di controllo.* • Audit: Write/Print + *Le azioni Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename e Create new, nomi dei file e flag (Write, DirectWrite, Format, Del, DirCreate) sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *I file sono scritti nel registro di shadowing.* • Shadowing: Write Non-files —
Hard disk	• Audit: Read + *Le azioni Open, Mount, Unmount e Direct Access, nomi dei file e flag (Read, DirectRead, Eject, DirList) sono scritti nel registro di controllo.*

TIPO DI PERIFERICA	DIRITTI
	• Audit: Write/Print + *Le azioni Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename e Create new, nomi dei file e flag (Write, DirectWrite, Format, Del, DirCreate) sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
Infrared port	• Audit: Read + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Write/Print + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
iPhone	• Audit: Read + *L'azione Read File e i nomi dei file vengono scritti nel registro di controllo*. • Audit: Write/Print + *Le azioni Write File, Rename File e Delete File e i nomi dei file vengono scritti nel registro di controllo*. • Audit: Execute — • Audit: Read Non-files + *Le azioni Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Backup, Read Note e Read Media e i nomi degli oggetti vengono scritti nel registro di controllo*. • Audit: Write Non-files + *Le azioni Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-mail, Write Backup, Write Note, Delete Note, Write Media, Rename Media e Delete Media e i nomi degli oggetti vengono scritti nel registro di controllo*. • Audit: Copy — • Shadowing: Write/Print + *I file vengono scritti nel registro di controllo*. • Shadowing: Write Non-files + *Tutti i dati contenenti oggetti diversi dai file (calendari, contatti, ecc.) vengono scritti nel registro di controllo*.

TIPO DI PERIFERICA	DIRITTI
Palm	• Audit: Read + *Scrittura di azione Read File, nomi file e flag Sync nel registro di controllo.* • Audit: Write/Print + *Scrittura di azione Write File nomi file e flag Sync nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files + *Scrittura di azioni Read Calendar, Read Contact, Read Expense, Read E-mail, Read Document, Read Memo, Read Notepad, Read Task e Read Media e nomi di oggetto nel registro di controllo.* • Audit: Write Non-files + *Scrittura di azioni Write Calendar, Write Contact, Write Expense, Write E-mail, Write Document, Write Memo, Write Notepad, Write Task, Write Media e Install e nomi di oggetto nel registro di controllo.* • Audit: Copy — • Shadowing: Write/Print + *I file vengono scritti nel registro di shadowing.* • Shadowing: Write Non-files + *Tutti i dati che contenuti in oggetti diversi dai file (Calendario, Contatti, Attività, ecc.) vengono scritti nel registro di shadowing*.
Parallel port	• Audit: Read + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Write/Print + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *Tutti i dati inviati alla porta sono scritti nel registro di shadowing.* • Shadowing: Write Non-files —
Printer	• Audit: Read — • Audit: Write/Print + *Scrittura di azione Print , documenti e nomi stampanti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *Tutti i dati inviati alla stampante vengono scritti nel registro di shadowing nel formato di spooler di stampa nativo.*

TIPO DI PERIFERICA	DIRITTI
	• Shadowing: Write Non-files —
Removable	• Audit: Read + *Le azioni Open, Mount, Unmount e Direct Access, nomi dei file e flag (Read, DirectRead, Eject, DirList) sono scritti nel registro di controllo.* • Audit: Write/Print + *Le azioni Open, Open/Create, Overwrite/Create, Direct Access, Delete, Rename e Create new, nomi dei file e flag (Write, DirectWrite, Format, Del, DirCreate) sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *I file sono scritti nel registro di shadowing.* • Shadowing: Write Non-files —
Serial port	• Audit: Read + *Le azioni Mount, Unmount, Insert, Remove e Device Access sono scritte nel registro di controllo.* • Audit: Write/Print + *Le azioni Mount, Unmount, Insert, Remove e Device Access sono scritte nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print + *Tutti i dati inviati alla porta sono scritti nel registro di shadowing.* • Shadowing: Write Non-files —
Tape	• Audit: Read + *Le azioni Open, Device Access e Direct Access e i flag (Read, DirectRead) sono scritti nel registro di controllo.* • Audit: Write/Print + *Le azioni Open, Device Access e Direct Access e i flag (Write, DirectWrite) sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
USB port	• Audit: Read + *Le azioni Insert, Remove e Device Access e i nomi delle periferiche*

TIPO DI PERIFERICA	DIRITTI
	sono scritti nel registro di controllo. • Audit: Write/Print + *Le azioni Insert, Remove e Device Access e i nomi delle periferiche sono scritti nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
WiFi	• Audit: Read + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Write/Print + *L'azione Device Access è scritta nel registro di controllo.* • Audit: Execute — • Audit: Read Non-files — • Audit: Write Non-files — • Audit: Copy — • Shadowing: Write/Print — • Shadowing: Write Non-files —
Windows Mobile	• Audit: Read + *Le azioni Read File, Get File Attributes, Create New File, Overwrite/Create File, Open File e Open/Create File, nomi dei file e flag sono scritti nel registro di controllo.* • Audit: Write/Print + *Le azioni Write File, Delete File, Rename File, Create File, Create New File, Overwrite/Create File, Open File, Open/Create File, Overwrite, Set File Attributes, Create Shortcut e Copy File, nomi dei file e flag sono scritti nel registro di controllo.* • Audit: Execute + *Le azioni Invoke e Execute, nomi dei file e nomi di funzioni (procedure) sono scritti nel registro di controllo*. • Audit: Read Non-files + *Le azioni Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Attachment, Read Note, Read Task, Read Media, Read Pocket Access e Read Unknown e i nomi degli oggetti sono scritti nel registro di controllo.* • Audit: Write Non-files + *Le azioni Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-Mail, Write Attachment, Delete Attachment, Write Note, Delete Note, Write Task, Delete Task, Write Media, Delete Media, Write Pocket Access, Delete Pocket Access, Write Unknown e Delete Unknown e i nomi degli oggetti sono scritti nel registro di controllo.* • Audit: Copy —

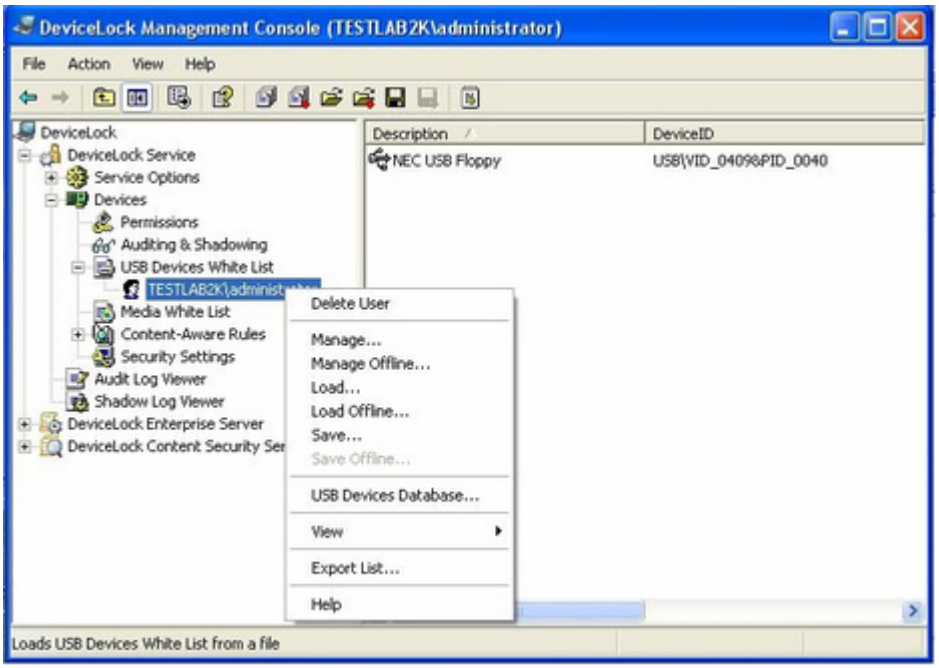
TIPO DI PERIFERICA	DIRITTI
	• Shadowing: Write/Print + *I file sono scritti nel registro di shadowing.* • Shadowing: Write Non-files + *Tutti i dati contenuti in oggetti diversi dai file (Calendario, Contatti, Attività, ecc.) vengono scritti nel registro di shadowing*.

Nota: anche se sono state definite le regole di controllo per una determinata periferica, per attivare la registrazione degli eventi, è necessario selezionare la casella di controllo **Audit Allowed** o **Audit Denied**.

Non è possibile registrare le azioni effettuate sulle periferiche elencate nella white list e le azioni effettuate su un'intera classe di periferiche qualora il controllo di accesso per tale classe è stato disattivato nelle impostazioni di protezione.

Sezione USB Devices White List (Regular Profile)

Questa white list consente di autorizzare l'utilizzo solo di determinate periferiche, indipendentemente dai parametri di protezione impostati. Lo scopo è di garantire il regolare utilizzo solo di determinate periferiche e, nello stesso tempo, di impedire l'utilizzo di tutte le altre periferiche.



Le periferiche elencate nella white list possono essere definite individualmente per ciascun utente e gruppo. Per ulteriori informazioni sulle white list, leggere la sezione Controllo dell'accesso gestito.

Nota: il controllo non viene eseguito per i tentativi degli utenti di accesso a una periferica autorizzata, mentre viene eseguito per i tentativi degli utenti di inserimento o rimozione di un dispositivo autorizzato.

L'identificazione delle periferiche elencate nella white list può essere eseguita in due modi:

- **Device Model** – rappresenta tutte le periferiche appartenenti ad uno stesso modello. Ciascuna periferica è identificata in base alla combinazione dei codici ID produttore (VID - Vendor ID) e ID prodotto (PID - Product ID).
  La combinazione degli identificatori VID e PID descrive in modo univoco un modello di periferica ma non un modello di unità. Ciò significa che tutte le periferiche appartenenti ad un determinato produttore vengono riconosciute come un'unica periferica autorizzata.

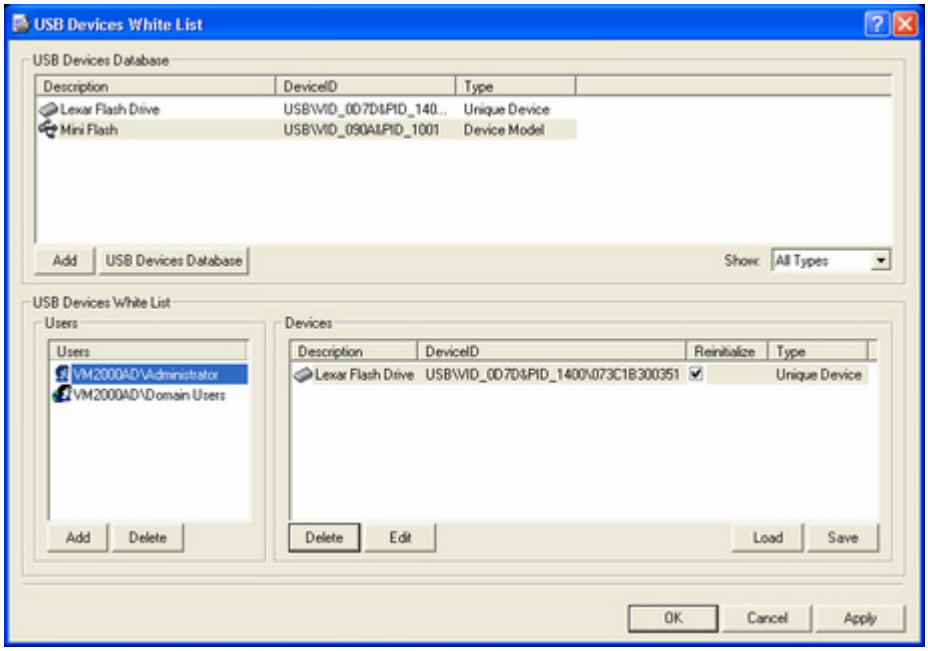
- **Unique Device** – rappresenta una unità di periferica univoca. Ciascuna periferica è identificata in base alla combinazione dei codici ID produttore (VID - Vendor ID), ID prodotto (PID - Product ID) e il numero di serie (SN).
  Non tutte le periferiche dispongono di un numero di serie. È possibile assegnare una periferica alla white list come periferica univoca (**Unique Device**) solamente se a questa il produttore, in fase di costruzione, ha assegnato un numero di serie.

Per consentire l'utilizzo di una periferica, è necessario eseguire due passaggi:

1. Aggiungere la periferica al database delle periferiche, in modo da poterla successivamente includere nella white list.
2. Aggiungere la periferica alla white list per l'utente o gruppo di utenti specificato. Questa operazione consente a tale utente o gruppo di utenti di utilizzare la periferica a livello di interfaccia (USB).

Nota: è possibile definire diverse liste bianche delle periferiche USB online od offline per lo stesso utente o gli stessi gruppi di utenti. La lista bianca delle periferiche USB online (Regular Profile) si applica ai computer client che operano online. La lista bianca delle periferiche USB offline (Offline Profile) si applica ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire la lista bianca delle periferiche USB offline, consultare la sezione "Gestione della lista bianca delle periferiche USB offline".

Per definire la white list, selezionare **Manage** dal menu contestuale richiamabile con il pulsante destro del mouse. In alternativa, fare clic sul relativo pulsante sulla barra degli strumenti.



L'elenco **USB Devices Database**, visibile nella parte superiore della finestra di dialogo, elenca le periferiche che sono state aggiunte al database.

Una volta che le periferiche vengono aggiunte dal database alla white list di un determinato utente, diventano periferiche autorizzate. Quando l'utente accede al sistema, il controllo dell'accesso per tali periferiche viene disattivato.

È possibile aggiungere una periferica alla white list in due passaggi:

1. Selezionare un utente o un gruppo di utenti a cui concedere l'accesso alla periferica. Per aggiungere un utente o un gruppo di utenti, fare clic sul pulsante **Add** visibile sotto l'elenco **Users**. Per rimuovere un utente o un gruppo di utenti dall'elenco **Users**, fare clic sul pulsante **Delete**.
2. Selezionare la periferica appropriata dall'elenco **USB Devices Database** e quindi fare clic sul pulsante **Add**.

   Se la periferica dispone di un numero di serie, può essere aggiunta due volte alla white list, sia come Device Type, sia come Unique Device. In questo caso, la periferica Device Type ha la priorità sulla periferica Unique Device.

Se il flag **Control as Type** è selezionato, il controllo degli accessi per le periferiche inserite nella white list è disattivato solo a livello di interfaccia (USB). Se la periferica elencata nella white list (ad esempio un'unità flash USB) appartiene a entrambi i livelli: interfaccia (USB) e tipo (Removable), si applicano comunque le eventuali autorizzazioni per il livello di tipo.

In caso contrario, se il flag **Control as Type** è deselezionato, è disattivato anche il controllo degli accessi a livello di tipo. Ad esempio, disattivando il flag **Control as Type** per l'unità flash USB è possibile ignorare il controllo di protezione a livello Removable.

Nota: se si aggiunge una periferica USB composita (rappresentata nel sistema da una periferica composita principale e una o più periferiche di interfaccia secondarie) nella lista bianca delle periferiche USB, considerare quanto segue:

Se si aggiunge qualsiasi periferica di una periferica USB composita nella lista bianca, il controllo dell'accesso viene disattivato per tutte le periferiche della periferica composita a livello di interfaccia (porta USB). Se la periferica inserita nella lista bianca appartiene a entrambi i livelli: interfaccia e tipo (ad esempio, rimovibile) e la casella di controllo **Control as Type** viene selezionata, le autorizzazioni (se presenti) per il livello del tipo vengono comunque applicate.

Se risulta necessario reinizializzare (replug) le periferiche elencate nella white list quando un nuovo utente si collega al sistema, selezionare la casella di controllo **Reinitialize**.

Poiché alcune periferiche USB (quali i mouse) non funzionano se non vengono reinizializzate, si consiglia di selezionare sempre questa casella di controllo.

Si raccomanda di non selezionare la casella di controllo **Reinitialize** per le periferiche di archiviazione, quali unità flash, CD/DVD-ROM, dischi fissi esterni e così via.

Alcune periferiche USB non possono essere reinizializzate da DeviceLock Service poiché i relativi driver non supportano la reinizializzazione via software. Se nella white list è presente una periferica di questo tipo e la periferica non funziona, per riavviare il driver della periferica è necessario che l'utente rimuova la periferica dalla porta e la inserisca manualmente nuovamente.

Per modificare la descrizione di una periferica, selezionarla nell'elenco **USB Devices White List** e scegliere **Edit**.

Per eliminare la periferica selezionata in elenco, fare clic sul pulsante **Delete** (per rimuovere più periferiche, utilizzare i tasti Ctrl e/o Maiusc).

Per salvare la white list in un file esterno, fare clic sul pulsante **Save** e quindi selezionare il nome del file. Per caricare una white list precedentemente salvata, fare clic sul pulsante **Load** e selezionare un file in cui è memorizzato l'elenco delle periferiche.

Per gestire il database delle periferiche, fare clic sul pulsante **USB Devices Database** e aprire la finestra di dialogo appropriata.

Nota: se si aggiunge un dispositivo iPhone alla lista bianca delle periferiche USB, il controllo dell'accesso viene disattivato per l'iPhone e per la sua telecamera a livello di interfaccia (porta USB). Di conseguenza, non è possibile autorizzare l'accesso all'iPhone e negare l'accesso alla sua telecamera a livello di interfaccia (porta USB). Nel database delle periferiche USB, un dispositivo iPhone viene identificato come “Apple Mobile Device USB Driver”.

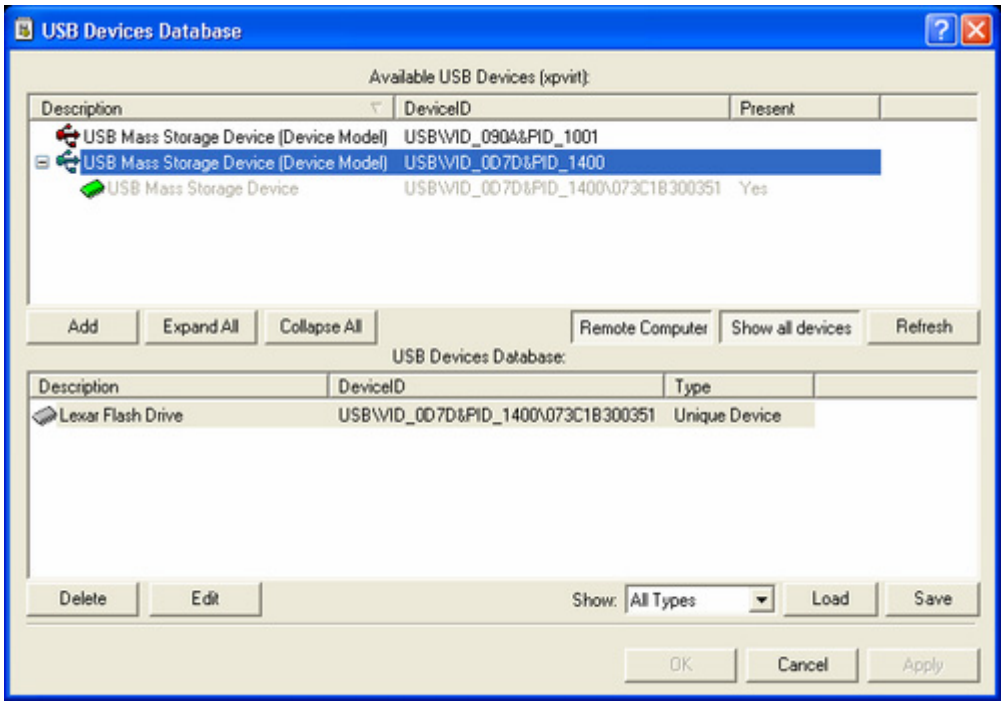
Tuttavia, è possibile autorizzare l'accesso alla telecamera dell'iPhone e negare l'accesso all'iPhone. Per farlo, è possibile ricorrere a uno qualsiasi dei seguenti metodi:

Metodo 1. Per autorizzare l'accesso alla telecamera dell'iPhone, aggiungere l'iPhone alla lista bianca delle periferiche USB e selezionare la casella di controllo **Control as Type**. Per negare l'accesso all'iPhone, impostare l'autorizzazione "No Access" per il tipo di periferica **iPhone**.

Metodo 2. Per autorizzare l'accesso alla telecamera dell'iPhone, deselezionare la casella di controllo **Access control for USB scanners and still image devices** in **Security Settings**. Per negare l'accesso all'iPhone, impostare l'autorizzazione "No Access" per il tipo di periferica **USB port**.

Sezione USB Devices Database

Nella finestra di dialogo **USB Devices Database** è possibile aggiungere nuove periferiche al database e modificare gli elementi già presenti in elenco.



Prima di poter autorizzare una periferica elencata nella white list, è necessario aggiungerla al database.

L'elenco **Available USB Devices**, visualizzato nella parte superiore della finestra di dialogo, mostra tutte le periferiche disponibili nel computer.

Le periferiche sono elencate in una semplice struttura ad albero, dove l'oggetto padre rappresenta il modello della periferica (**Device Model**) e l'oggetto figlio rappresenta la periferica univoca (**Unique Device**). Se l'oggetto **Unique Device** non è presente, la relativa periferica non dispone di un numero di serie.

Se si seleziona il pulsante **Show all devices**, DeviceLock visualizzerà tutte le periferiche che sono state collegate alla porta del computer. Se si deseleziona il pulsante **Show all devices**, DeviceLock elencherà solamente le periferiche correntemente collegate alla porta del computer. DeviceLock aggiorna automaticamente l'elenco delle periferiche disponibili non appena una nuova periferica viene collegata al computer. Per aggiornare manualmente le voci presenti in elenco, fare clic sul pulsante **Refresh**.

Per ottenere l'elenco delle periferiche da un computer remoto, fare clic sul pulsante **Remote Computer**. Questo pulsante non è disponibile quando si è connessi al computer locale.

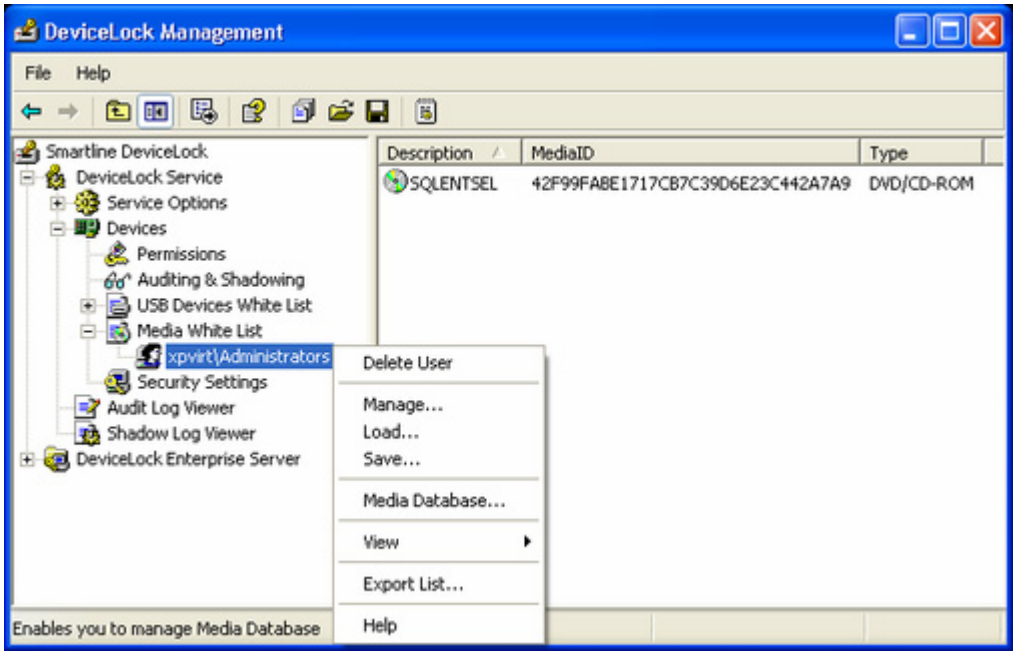
L'elenco inferiore **USB Devices Database** visualizza le periferiche già presenti nel database.

Per aggiungere una periferica in questo elenco, selezionare la periferica desiderata nell'elenco **Available USB Devices**, quindi fare clic sul pulsante **Add**. Non è possibile aggiungere più di una volta la stessa periferica. Per modificare la descrizione di una periferica, selezionarla nell'elenco **USB Devices Database**, quindi fare clic sul pulsante **Edit**. Per eliminare una periferica, selezionarla, quindi fare clic sul pulsante **Delete** (per selezionare più periferiche contemporaneamente, utilizzare i tasti CTRL e/o MAIUSCOLO).

Se si desidera salvare il database corrente in un file esterno, fare clic sul pulsante **Save**, quindi scegliere il tipo di file da creare (documento di testo con estensione txt o documento di testo delimitato da separatore di elenco con estensione csv). Per aprire un database precedentemente salvato, fare clic sul pulsante **Load**, quindi selezionare il file contenente l'elenco delle periferiche.

Sezione Media White List (Regular Profile)

Questa white list consente di identificare in modo univoco un determinato disco DVD/CD-ROM, in base alla firma dei dati in esso contenuti. Consente inoltre di concedere l'accesso in sola lettura al supporto, perfino quando le unità DVD/CD-ROM sono bloccate da DeviceLock Service.



È possibile configurare la white list in modo da concedere solo agli utenti autorizzati l'accesso alle informazioni contenute in un gruppo di dischi DVD/CD-ROM che dispongono di autorizzazioni di lettura.

La modifica del contenuto dei supporti multimediali comporta la modifica della firma dei dati e, di conseguenza, l'invalidazione dell'autorizzazione. Se l'utente copia il supporto autorizzato senza apportare modiche al contenuto originale (ovvero, effettua una copia byte-a-byte), tale copia viene accettata come autorizzata.

Nota: l'accesso ai supporti multimediali elencati nella white list può essere concesso solo a livello di tipo (DVD/CD-ROM). Se l'unità DVD/CD è collegata ad una porta (USB o FireWire) a cui è negato l'accesso, non sarà possibile accedere al contenuto del supporto multimediale elencato nella white list.

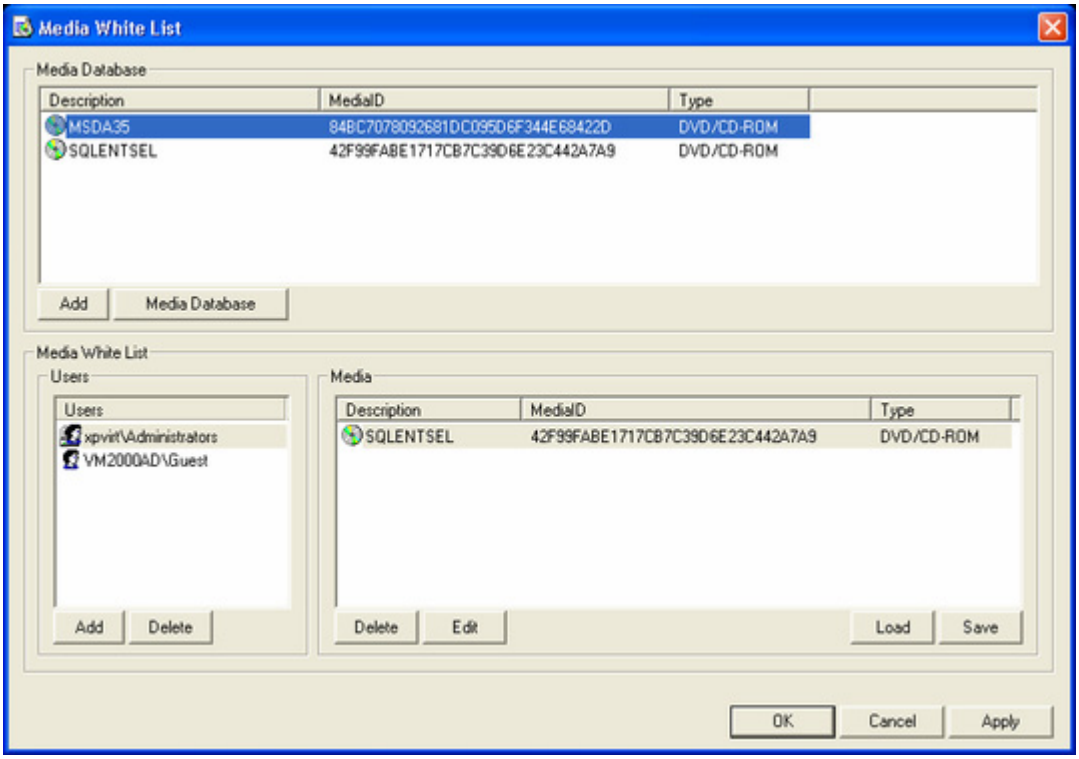
Per autorizzare un supporto multimediale, è necessario eseguire due passaggi:

1. Aggiungere il supporto multimediale al database dei supporti multimediali, in modo da poterlo successivamente includere nella white list.
2. Aggiungere il supporto multimediale alla white list per l'utente o gruppo di utenti specificato. Questa operazione autorizza il supporto multimediale e concede all'utente o al gruppo di utenti l'accesso (in sola lettura) ad esso a livello di tipo (DVD/CD-ROM).

Nota: è possibile definire diverse liste bianche delle unità online od offline per lo stesso utente o gli stessi gruppi di utenti. La lista bianca delle unità online (Regular Profile) si applica ai computer client che operano online. La lista bianca delle unità offline (Offline Profile) si applica ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione

DeviceLock (Offline Profile)". Per informazioni su come definire la lista bianca delle unità offline, consultare la sezione "Gestione della lista bianca delle unità offline".

Per definire una white list di supporti multimediali, selezionare **Manage** dal menu contestuale richiamabile con il pulsante destro del mouse. In alternativa, fare clic sul relativo pulsante della barra degli strumenti.



L'elenco **Media Database**, visibile nella parte superiore della finestra di dialogo, elenca i supporti multimediali che sono state aggiunti al database.

Una volta che i supporti multimediali vengono aggiunti dal database alla white list di un determinato utente, diventano dischi autorizzati. Quando l'utente accede al sistema, il controllo dell'accesso per tali dischi viene disattivato.

È possibile aggiungere un supporto multimediale alla Media White List in due passaggi:

1. Selezionare un utente o un gruppo di utenti a cui concedere l'accesso al supporto multimediale. Per aggiungere un utente o un gruppo di utenti, fare clic sul pulsante **Add** visibile sotto l'elenco **Users**. Per rimuovere un utente o un gruppo di utenti dall'elenco **Users**, fare clic sul pulsante **Delete**.
2. Selezionare il supporto multimediale appropriato dall'elenco **Media Database** e quindi fare clic sul pulsante **Add**.

Per modificare la descrizione di un supporto multimediale, selezionarlo nell'elenco **Media White List** e scegliere **Edit**.

Per eliminare il supporto multimediale selezionato in elenco, fare clic sul pulsante **Delete** (per rimuovere più supporti multimediali, utilizzare i tasti Ctrl e/o Maiusc).

Per salvare la white list in un file esterno, fare clic sul pulsante **Save** e quindi selezionare il nome del file.

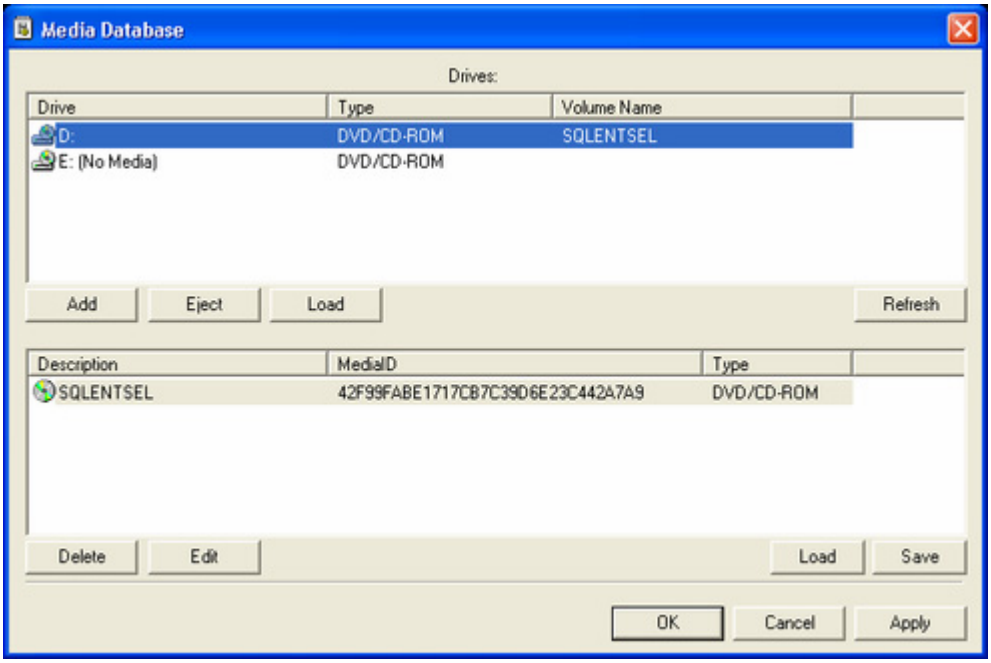
Per caricare una white list precedentemente salvata, fare clic sul pulsante **Load** e selezionare un file in cui è memorizzato l'elenco dei supporti multimediali.

Per gestire il database dei supporti multimediali, fare clic sul pulsante **Media Database** e aprire la finestra di dialogo appropriata.

Nota: la white list dei supporti multimediali consente solo di concedere l'accesso in lettura ai supporti multimediali autorizzati. Non è possibile concedere l'accesso in scrittura.

Finestra di dialogo Media Database

Nella finestra di dialogo **Media Database** è possibile aggiungere nuovi supporti multimediali al database e modificare gli elementi già presenti in elenco.



Prima di poter autorizzare un supporto multimediale elencato nella white list, è necessario aggiungerlo al database.

L'elenco **Drives**, visualizzato nella parte superiore della finestra di dialogo, mostra tutte le unità disponibili sul computer locale in grado di accedere ai supporti multimediali.

DeviceLock aggiorna automaticamente l'elenco dei supporti multimediali non appena viene riconosciuto un nuovo supporto multimediale. Per aggiornare manualmente le voci presenti in elenco, fare clic sul pulsante **Refresh**.

L'elenco inferiore visualizza i supporti multimediali già presenti nel database.

Per aggiungere un supporto multimediale in questo elenco, selezionare il supporto multimediale desiderato nell'elenco **Drives**, quindi fare clic sul pulsante **Add**. L'operazione di autorizzazione richiede del tempo, in base alla capacità del supporto multimediale. Non è possibile aggiungere più di una volta lo stesso supporto multimediale al database.

Per modificare la descrizione di un supporto multimediale, selezionarlo in elenco, quindi fare clic sul pulsante **Edit**.

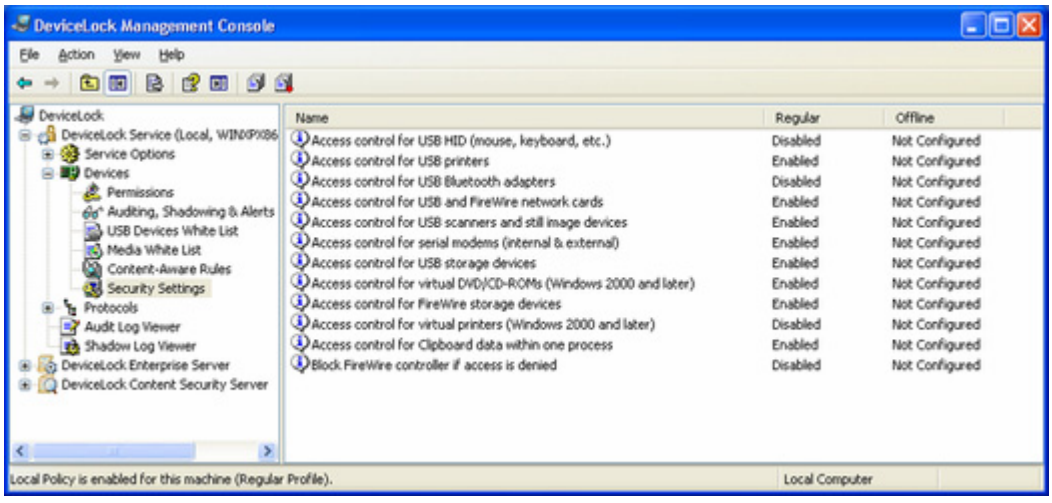
Per eliminare un supporto multimediale, selezionarlo, quindi fare clic sul pulsante **Delete** (per selezionare più supporti multimediali contemporaneamente, utilizzare i tasti CTRL e/o MAIUSCOLO).

Se si desidera salvare il database corrente in un file esterno, fare clic sul pulsante **Save**, quindi scegliere il tipo di file da creare (documento di testo con estensione txt o documento di testo delimitato da separatore di elenco con estensione csv).

Per aprire un database precedentemente salvato, fare clic sul pulsante **Load**, quindi selezionare il file contenente l'elenco dei supporti multimediali.

Sezione Security Settings (Regular Profile)

È possibile definire ulteriori parametri di protezione che influenzano le autorizzazioni e le regole di controllo di alcuni tipi di periferica.


DeviceLock Management Console
File Action View Help
DeviceLock
DeviceLock Service (Local, WINDPX86
Service Options
Devices
Permissions
Auditing, Shadowing & Alerts
USB Devices White List
Media White List
Content-Aware Rules
Security Settings
Protocols
Audit Log Viewer
Shadow Log Viewer
DeviceLock Enterprise Server
DeviceLock Content Security Server
Name
Regular
Offline
Access control for USB HID (mouse, keyboard, etc.) Disabled Not Configured
Access control for USB printers Enabled Not Configured
Access control for USB Bluetooth adapters Disabled Not Configured
Access control for USB and FireWire network cards Enabled Not Configured
Access control for USB scanners and still image devices Enabled Not Configured
Access control for serial modems (internal & external) Enabled Not Configured
Access control for USB storage devices Enabled Not Configured
Access control for virtual DVD/CD-ROMs (Windows 2000 and later) Enabled Not Configured
Access control for FireWire storage devices Enabled Not Configured
Access control for virtual printers (Windows 2000 and later) Disabled Not Configured
Access control for Clipboard data within one process Enabled Not Configured
Block FireWire controller if access is denied Disabled Not Configured
Local Policy is enabled for this machine (Regular Profile).
Local Computer

Grazie a questi parametri di protezione, è possibile tenere completamente bloccati alcuni tipi di periferica e, al contempo, concedere l'utilizzo di determinate classi di periferica senza la necessità di dover autorizzare ciascuna periferica nella white list.

Ad esempio, è possibile negare l'utilizzo di tutte le periferiche USB ad eccezione del mouse USB e della tastiera USB.

DeviceLock supporta tre parametri di protezione addizionali:

- **Access control for USB HID** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso alle periferiche HID (quali mouse, tastiera e così via) collegate alla porta USB. Se l'opzione non è attivata, DeviceLock Service non controllerà le periferiche HID e queste continueranno a funzionare regolarmente, anche se collegate ad una porta USB bloccata.
- **Access control for USB printers** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso alle stampanti collegate alla porta USB. Se l'opzione non è attivata, DeviceLock Service non controllerà tali periferiche e queste continueranno a funzionare regolarmente, anche se collegate ad una porta USB bloccata.
- **Access control for USB scanners and still image devices** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso agli scanner e alle periferiche di acquisizione immagini collegati alla porta USB. Se l'opzione non è attivata, DeviceLock Service non controllerà tali periferiche e queste continueranno a funzionare regolarmente, anche se collegate ad una porta USB bloccata.
- **Access control for USB Bluetooth adapters** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso ai dispositivi Bluetooth collegati alla porta USB. Se l'opzione non è attivata, DeviceLock Service non controllerà i dispositivi Bluetooth e tali dispositivi continueranno a funzionare regolarmente, anche se collegati ad una porta USB bloccata.

  Questo parametro influenza il controllo degli accessi solamente a livello di interfaccia (USB). Se il controllo degli accessi alla periferica avviene sia a livello di interfaccia, sia a livello di tipo, vengono comunque applicate le autorizzazioni assegnate a livello di tipo (Bluetooth), se presenti.

- **Access control for USB storage devices** – se l'opzione è attivata, DeviceLock Service controllerà gli accessi alle periferiche di archiviazione (quale un'unità flash) collegate alla porta USB. Se l'opzione non è attivata, DeviceLock Service non controllerà le periferiche di archiviazione e queste continueranno a funzionare correttamente, anche se sono collegate ad una porta USB bloccata.

  Questo parametro influenza il controllo degli accessi solamente a livello di interfaccia (USB). Se il controllo degli accessi alla periferica avviene sia a livello di interfaccia, sia a livello di tipo, vengono comunque applicate le autorizzazioni assegnate a livello di tipo (Removable, Floppy, DVD/CD-ROM oppure Hard disk).

- **Access control for USB and FireWire network cards** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso a schede di rete collegate alla porta FireWire (IEEE 1394) o USB. Se l'opzione non è attivata, DeviceLock Service non controllerà le schede di rete e queste continueranno a funzionare regolarmente, anche se collegate ad una porta FireWire o USB bloccata.
- **Access control for FireWire storage devices** – se l'opzione è attivata, DeviceLock Service controllerà gli accessi alle periferiche di archiviazione collegate alla porta FireWire. Se l'opzione non è attivata, DeviceLock Service non controllerà le periferiche di archiviazione e queste continueranno a funzionare correttamente, anche se sono collegate ad una porta FireWire bloccata.

  Questo parametro influenza il controllo degli accessi solamente a livello di interfaccia (FireWire). Se il controllo degli accessi alla periferica avviene sia a livello di interfaccia, sia a livello di tipo, vengono comunque applicate le autorizzazioni assegnate a livello di tipo (Removable, Floppy, DVD/CD-ROM oppure Hard disk).

- **Access control for serial modems (internal & external)** – se l'opzione è attivata, DeviceLock Service controllerà l'accesso ai modem collegati alle porte COM. Se l'opzione non è attivata, DeviceLock Service non controllerà i modem e questi continueranno a funzionare regolarmente, anche se collegati a porte COM bloccate.
- **Access control for virtual CD-ROMs** – se l'opzione è attivata, DeviceLock Service controllerà gli accessi effettuati alle unità CD-ROM virtuali emulate via software. Se l'opzione non è attivata, DeviceLock Service non controllerà le unità virtuali e queste continueranno a funzionare regolarmente, anche se l'unità CD-ROM è bloccata. Questo parametro è valido solo per i computer che eseguono Windows 2000 e versioni successive.
- **Access control for virtual printers** – se selezionato, consente a DeviceLock Service di controllare l'accesso alle stampanti virtuali che non inviano documenti verso periferiche reali, ma che inviano stampe su file (p. es. convertitori PDF). In caso contrario, anche se la stampante fisica è bloccata, le stampanti virtuali continuano a stampare normalmente e non vengono sottoposte a controllo. Questo parametro risulta effettivo solo sui sistemi operativi Windows 2000 e versioni successive.
- **Access control for inter-application copy/paste clipboard operations** - se attivata, consente a DeviceLock Service di controllare e verificare l'accesso alle operazioni copia/incolla tra diverse applicazioni. In caso contrario, anche se gli Appunti sono bloccati, il controllo dell'accesso per le operazioni di copia/incolla tra diverse applicazioni risulta disattivato e non viene eseguita alcuna verifica.
- **Block FireWire controller if access is denied** – se attivata, questa opzione consente a DeviceLock Service di disattivare i controller FireWire quando l'account Everyone dispone delle autorizzazioni No Access per il tipo di periferica porta FireWire.

Nota: è possibile definire diverse impostazioni di protezione online od offline per lo stesso utente o gli stessi gruppi di utenti. Le impostazioni di protezione online (Regular Profile) si applicano ai computer client che operano online. Le impostazioni di protezione offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come impostare le impostazioni di protezione offline, consultare la sezione "Gestione delle impostazioni di protezione offline".

Per modificare lo stato (attivato/disattivato) di un parametro di protezione, fare doppio clic su di esso. In alternativa, selezionare **Manage** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual DVD/CD-ROMs (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
Access control for Clipboard data within one process
Block FireWire controller if access is denied
OK
Cancel

Le impostazioni di protezione sono simili alla white list delle periferiche, sebbene presentino tre differenze sostanziali:

1. Le impostazioni di protezione consentono di definire le autorizzazioni solo per una classe completa di periferiche. In una stessa classe di periferiche, non è possibile quindi concedere l'uso di una periferica e, al contempo, bloccare l'accesso alle periferiche rimanenti.

   Ad esempio, se si disattiva il parametro **Access control for USB storage devices**, sarà possibile utilizzare tutte le periferiche di archiviazione USB, indipendentemente dal modello e dal produttore. Se nella white list delle periferiche si autorizza l'utilizzo di un modello di unità flash USB, ci si assicura che le rimanenti periferiche di archiviazione USB rimarranno bloccate.

2. Le impostazioni di protezione consentono di selezionare una periferica solamente se questa appartiene ad una delle classi di periferiche predefinite. In caso contrario, non è possibile concedere l'uso della periferica.

   Ad esempio, nelle impostazioni di protezione non esistono classi specifiche per i lettori di smart card. Quindi, se si desidera autorizzare un lettore di smart card collegato ad una porta bloccata, è necessario utilizzare la white list.

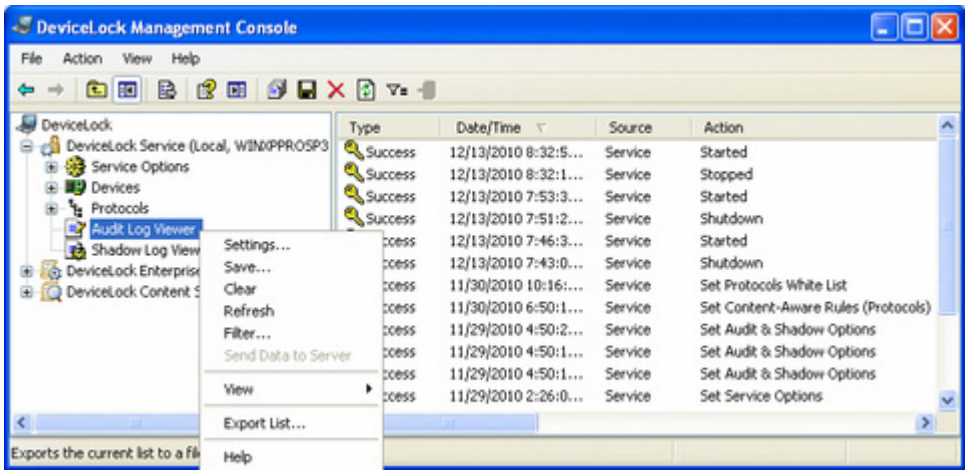
3. Le impostazioni di protezione non possono essere definite in base a criteri personalizzabili per singolo utente, ma hanno effetto su tutti gli utenti del computer locale. Le periferiche incluse nella white list, invece, possono essere definite individualmente per ogni utente e gruppo di utenti.

Nota: le impostazioni di protezione funzionano solamente con le periferiche che utilizzano i driver standard di Windows. Alcune periferiche utilizzano dei driver proprietari e la relativa classe di appartenenza non può essere riconosciuta da DeviceLock Service. Di conseguenza, non è possibile disattivare il controllo di accesso per tali periferiche tramite le impostazioni di protezione. In questo caso, per autorizzare una periferica, è necessario utilizzare la white list.

Sezione Audit Log Viewer (Servizio)

DeviceLock Management integra un visualizzatore di eventi in grado di visualizzare gli eventi di controllo di DeviceLock registrati nel sottosistema standard di registrazione degli eventi di Windows.

Per memorizzare gli eventi di controllo, DeviceLock utilizza il sottosistema standard di registrazione degli eventi di Windows, ma solamente se l'opzione **Event Log** oppure **Event & DeviceLock Logs** è selezionata nelle impostazioni del servizio. Altrimenti, gli eventi di controllo vengono memorizzati in un registro proprietario e possono essere visualizzati con il visualizzatore degli eventi del server.



DeviceLock memorizza negli eventi di controllo gli eventi generati dalle attività effettuate da un utente su una periferica, in base alle regole di controllo impostate. Per ulteriori informazioni, leggere Sezione Auditing & Shadowing.

Se si seleziona la relativa opzione nelle impostazioni del servizio, nel registro eventi di controllo vengono memorizzate anche le modifiche apportate alla configurazione di DeviceLock Service.

Il visualizzatore di eventi mostra le seguenti informazioni:

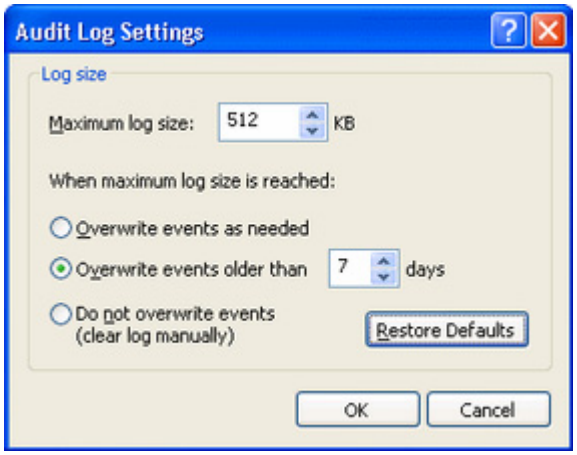
- **Type** – la classe di un evento. Può assumere il valore **Success** se l'accesso è stato consentito o **Failure** se l'accesso è stato bloccato.
- **Date/Time** – la data e l'ora in cui si è verificato l'evento.
- **Source** - il tipo di periferica o protocollo coinvolto.
- **Action** – il tipo di attività effettuata dall'utente.
- **Name** – il nome dell'oggetto (file, periferica USB e così via).
- **Information** – informazioni sull'evento relative alla periferica, quali i flag di accesso, il nome della periferica USB e così via.
- **User** – il nome dell'utente associato all'evento.
- **PID** – l'identificativo del processo associato all'evento.
- **Process** – il percorso completo del file eseguibile (processo). In alcuni casi, in questa colonna è visualizzato il nome del processo anziché il percorso.

Per aggiornare il registro eventi, selezionare **Refresh** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Per cancellare il contenuto del registro, selezionare **Clear** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Sezione Audit Log Settings (Servizio)

Per definire la dimensione massima del file registro e specificare l'operazione da eseguire quando il registro diventa pieno, selezionare **Settings** dal menu contestuale richiamabile con il pulsante destro del mouse oppure facendo clic sul relativo pulsante sulla barra degli strumenti.



Il parametro **Maximum log size** specifica la dimensione massima del file registro (in kilobyte). Il file registro viene creato e utilizzato solo dal servizio Registro eventi di

Windows. Questo file viene generalmente memorizzato nella cartella ***%SystemRoot%\system32\config*** ed è nominato ***DeviceLo.evt***.

Per specificare l'operazione che deve eseguire Windows quando il file registro diventa pieno (ovvero, quando la dimensione del registro corrisponde al valore assegnato al parametro **Maximum log size**), selezionare una delle seguenti opzioni:

- **Overwrite events as needed** – il sistema sostituisce gli eventi meno recenti con quelli più recenti quando il registro è pieno, ovvero quando la dimensione del file registro corrisponde al valore assegnato al parametro **Maximum log size**.
- **Overwrite events older than** – specifica il numero di giorni in cui il file registro verrà mantenuto prima di essere sovrascritto.
- **Do not overwrite events (clear log manually)** – gli eventi esistenti verranno mantenuti quando il registro è pieno, ovvero quando la dimensione del file registro corrisponde al valore assegnato al parametro **Maximum log size**. È necessario cancellare manualmente il contenuto del file registro.

Nota: DeviceLock Service non potrà scrivere nuovi eventi nel file registro se questo è pieno e non esistono record che possono essere eliminati da Windows.

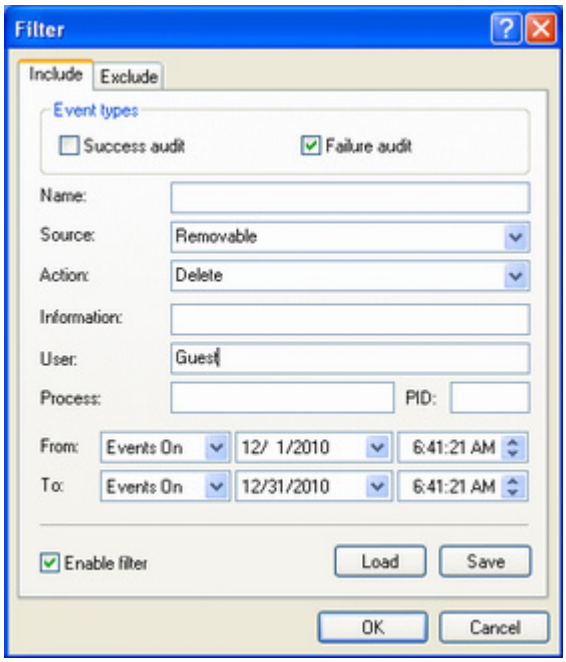
Per reimpostare i valori predefiniti delle impostazioni, fare clic sul pulsante **Restore Defaults**. I valori predefiniti sono i seguenti:

- il valore predefinito del parametro **Maximum log size** è 512 kilobyte.
- l'operazione predefinita è **Overwrite events older than** e il numero di giorni predefinito è 7.

Sezione Audit Log Filter (Servizio)

È possibile filtrare i dati elencati nel visualizzatore degli eventi di controllo in base a determinati criteri.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.



Esistono due tipi di filtri:

- **Include** – vengono mostrati solo gli eventi che soddisfano i criteri specificati nella scheda **Include**.
- **Exclude** – non vengono mostrati gli eventi che soddisfano i criteri specificati nella scheda **Exclude**.

Per applicare un filtro, è necessario prima attivarlo. Per attivare un filtro, selezionare la casella di controllo **Enable filter**. Per disattivare temporaneamente un filtro, deselezionare la casella di controllo **Enable filter**.

Quando un filtro è attivato, è possibile definirne i criteri impostando i seguenti campi:

- **Success audit** – specifica se visualizzare tentativi di accesso alla periferica riusciti.
- **Failure audit** – specifica se visualizzare tentativi di accesso alla periferica non riusciti.
- **Name** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Name** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Source** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Source** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).

- **Action** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Action** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Information** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Information** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **User** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **User** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Process** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Process** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **PID** – casella in cui digitare un numero che corrisponda a quello riportato nella colonna **PID** del visualizzatore di eventi.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **From** – specifica l'inizio dell'intervallo di eventi da filtrare. Selezionare **First Event** per visualizzare gli eventi a partire dal primo evento registrato. Selezionare **Events On** per visualizzare gli eventi che si sono verificati a partire da una data e da un'ora specifiche.
- **To** – specifica la fine dell'intervallo di eventi da filtrare. Selezionare **Last Event** per visualizzare gli eventi fino all'ultimo evento registrato. Selezionare **Events On** per visualizzare gli eventi che si sono verificati fino ad una data e ad un'ora specifiche.

L'operatore logico AND viene applicato a tutti i campi specificati e a tutti i filtri attivi (schede **Include**/**Exclude**). Ciò significa che il risultato del filtro include solamente i record che soddisfano tutti i criteri impostati.

Per non includere un campo nei criteri del filtro, lasciare il campo vuoto.

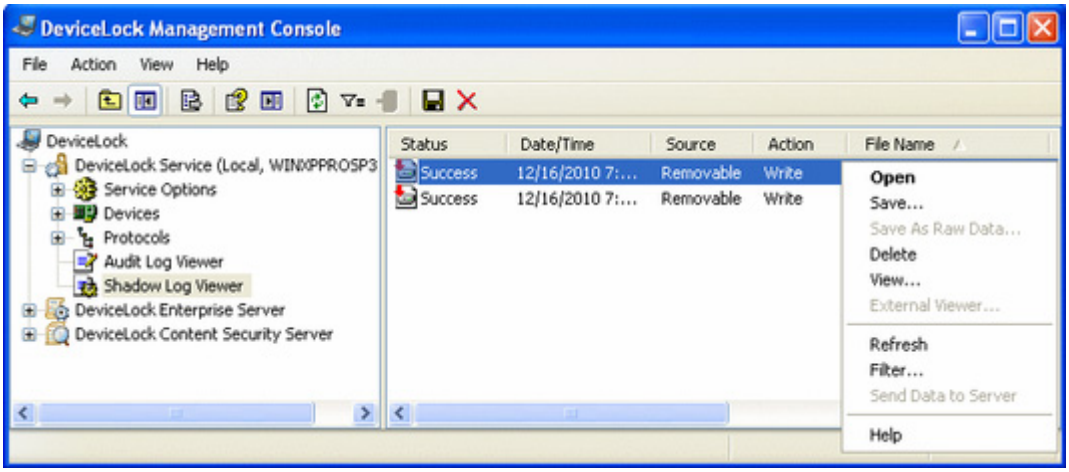
In alcuni campi è possibile utilizzare i caratteri jolly. Un carattere jolly è un carattere quale un asterisco (*) o un punto interrogativo (?) utilizzato per rappresentare uno o più caratteri nella definizione di un filtro.

Utilizzare l'asterisco come sostituto di zero o più caratteri. Se si sta cercando un nome che comincia con "win", ma di cui non si ricorda la parte rimanente, digitare: **win***. Questa stringa individua tutti i nomi che cominciano con "win", inclusi Windows, Winner, e Wind.

Utilizzare il punto interrogativo come sostituto di un singolo carattere in un nome. Ad esempio, se si digita **win?**, sarà individuato il nome Wind ma non saranno individuati i nomi Windows o Winner.

Sezione Shadow Log Viewer (Servizio)

DeviceLock Management integra un visualizzatore di eventi di shadowing in grado di visualizzare gli eventi di shadowing di DeviceLock Service.



Se si utilizza la configurazione tipica di DeviceLock, le copie shadow dei dati vengono memorizzate sul computer in cui è installato DeviceLock Enterprise Server. In questo caso, tutte le copie shadow dei dati che sono state originariamente memorizzate nel file registro di DeviceLock Service sul computer locale vengono periodicamente spostate sul server. Il file registro di shadowing locale viene reimpostato non appena i dati risultano correttamente spostati sul server. Per visualizzare questi dati, utilizzare il visualizzatore di eventi del server.

In alcuni casi, può essere utile visualizzare gli eventi di shadowing di un determinato computer, ad esempio quando non si utilizza DeviceLock Enterprise Server oppure quando il server è in uso, ma per qualche motivo i dati risiedono ancora sul computer client.

Il visualizzatore di eventi mostra le seguenti informazioni:

- **Status** – indica lo stato del record. Lo stato **Success** indica che i dati sono stati registrati correttamente, lo stato **Incomplete** indica che i dati non sono stati registrati completamente, mentre lo stato **Failed** viene associato alle copie shadow dei file la cui trasmissione è stata bloccata dalle regole basate sul contenuto (Content-Aware Rules).
- **Date/Time** – la data e l'ora in cui i dati sono stati trasferiti.
- **Source** - il tipo di periferica o protocollo coinvolto.
- **Action** – il tipo di attività dell'utente.

- **File Name** – il percorso originale del file o del nome assegnato automaticamente ai dati che in origine non erano file (ad esempio, i file immagine dei CD/DVD, i dati scritti direttamente su un supporto multimediale o i dati trasferiti tramite porta seriale/parallela).
- **File Size** – la dimensione dei dati.
- **User** – il nome dell'utente che ha trasferito i file.
- **PID** – l'identificativo del processo utilizzato per trasferire i dati.
- **Process** – il percorso completo del file eseguibile (processo). In alcuni casi, in questa colonna è visualizzato il nome del processo anziché il percorso.

Per eseguire i seguenti comandi, richiamare il menu contestuale facendo clic con il pulsante destro del mouse su ciascuna voce dell'elenco.

Comando "Open"
Per aprire il file da un record selezionato utilizzando l'applicazione a esso associata, scegliere **Open** dal menu contestuale. Se non è associata alcuna applicazione, viene visualizzata la finestra di dialogo "**Open With**". Se al record non è associato alcun dato (le sue dimensioni sono pari a 0 o non è stato registrato), il comando **Open** è disattivato.

Se si utilizza **Open** per i dati di shadowing acquisiti dai tipi di periferica Printer o Parallel port, l'applicazione associata è sempre il visualizzatore integrato DeviceLock Printer Viewer.

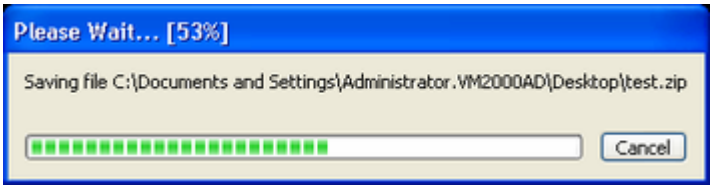
DeviceLock Printer Viewer è in grado di mostrare il documento di shadowing stampato nel formato di spooler di stampa nativo, di inviarlo nuovamente alla stampante o di salvarlo come file grafico (in formato BMP, GIF, JPEG, PNG, EMF o TIFF). Sono supportati i seguenti formati di spooler di stampa: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, stampa GDI (ZjStream) ed EMF Spooled Files.

Comando "Save"
Per salvare sul computer locale i dati relativi alla voce selezionata, scegliere **Save** dal menu contestuale oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Utilizzare i tasti Ctrl e/o Maiusc per evidenziare più voci e salvare contemporaneamente i relativi dati.

Se la voce in elenco non dispone di dati (la dimensione è 0 oppure non è stata registrata alcuna informazione), il comando **Save** sarà disattivato sia sul menu contestuale, sia sulla barra degli strumenti.

Durante il salvataggio di un file di grosse dimensioni, DeviceLock mostra una barra di avanzamento.



È possibile fare clic sul pulsante **Cancel** in qualsiasi momento per interrompere il processo di salvataggio. In tal caso, il file sul computer locale risulterà incompleto e conterrà solo una parte dei dati ricevuti prima dell'interruzione del salvataggio.

Se i dati sono stati trasferiti come file, questi sono memorizzati nel registro eventi di shadowing come file e possono essere salvati sul computer locale come file.

Quando un utente scrive i dati su un disco CD/DVD, tutti i dati vengono memorizzati nel registro eventi di shadowing come singolo file immagine CD/DVD in formato CUE (viene memorizzato un file immagine per ciascun disco CD/DVD scritto o per sessione).

Ai file immagine CD/DVD, così come ai dati che in origine non sono stati trasferiti come file (ad esempio, i dati trasferiti con accesso diretto ai dischi o trasferiti tramite porta seriale/parallela), viene assegnato un nome generato automaticamente e basato sul tipo di azione effettuata dall'utente, dalla lettera dell'unità o dal nome

della periferica e dalla data e dell'ora (ad esempio, direct_write(E:) 19:18:29 17.07.2006.bin).

Quando si salva un file immagine CD/DVD sul disco locale, vengono creati due file: il file dei dati con estensione .bin (ad esempio, direct_write(E_) 19_18_29 17_07_2006.bin) ed il file cue sheet, a cui viene assegnato lo stesso nome del file dei dati con estensione .cue (ad esempio, direct_write(E_) 19_18_29 17_07_2006_bin.cue). Entrambi i file sono necessari per aprire il file immagine CD/DVD con un'applicazione che supporta il formato CUE (quali Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO e molti altri).

Comando "Save As Raw Data"

Quando si seleziona una voce in elenco che contiene dati originariamente scritti come sessione addizionale in un disco multi-sessione CD/DVD, diventa disponibile il comando **Save As Raw Data** nel menu contestuale. Questo comando consente di salvare i dati sul computer locale così come sono, senza correggere i riferimenti ai dati memorizzati nelle sessioni precedenti.

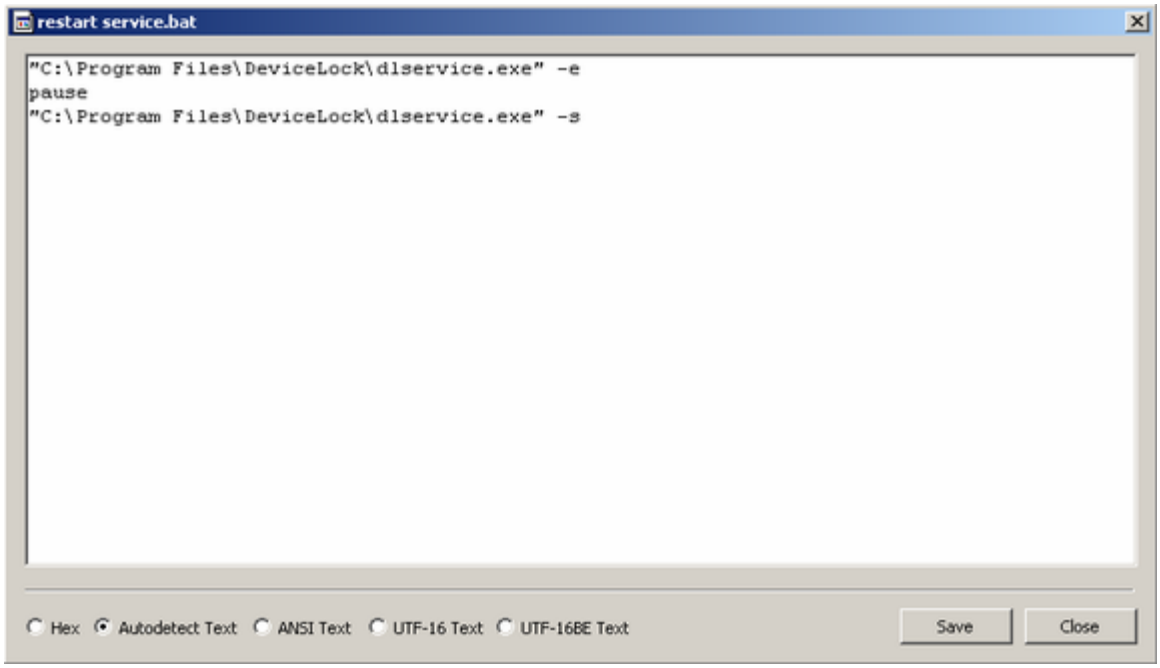
Se si utilizza la funzione standard di salvataggio **Save**, DeviceLock Management Console rileva che il file immagine CD/DVD contiene una sessione che fa riferimento ai dati memorizzati nelle sessioni precedenti. Poiché le sessioni precedenti non sono disponibili (potrebbero essere state scritte su un computer dove non è installato DeviceLock Service), DeviceLock Management Console trova e corregge tutti i riferimenti a queste sessioni non esistenti, in modo da creare un file .cue leggibile con le applicazioni che supportano questo formato.

Per ottenere i dati che non sono stati modificati da DeviceLock Management Console, scegliere **Save As Raw Data**. In questo caso, il file risultante potrebbe essere illeggibile alle applicazioni che supportano il formato CUE.

Quando si salvano file di grosse dimensioni, è possibile fare clic sul pulsante **Cancel** visibile a fianco della barra di avanzamento per interrompere l'operazione di salvataggio. In tal caso, il file sul computer locale risulterà incompleto e conterrà solo una parte dei dati ricevuti prima dell'interruzione del salvataggio.

Comando "View"

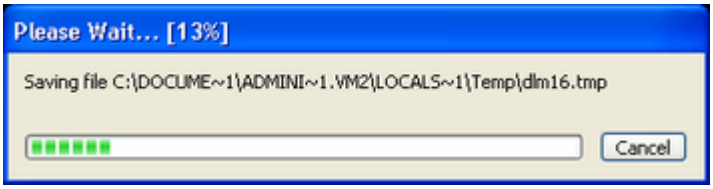
Per visualizzare il contenuto dei dati nel visualizzatore integrato, scegliere **View** dal menu contestuale.



Nel visualizzatore integrato, fare clic su una qualsiasi delle opzioni di visualizzazione seguenti:

- **Hex**: mostra i dati in formato hex e sotto forma di parole.
- **Autodetect Text**: attiva il rilevamento automatico della codifica per il testo e mostra i dati unicamente in formato testo.
- **ANSI Text**: specifica la codifica ANSI per il testo e mostra i dati unicamente in formato testo.
- **UTF-16 Text**: specifica la codifica Unicode UTF-16 per il testo e mostra i dati unicamente in formato testo.
- **UTF-16BE Text**: specifica la codifica Unicode UTF-16 (Big Endian) per il testo e mostra i dati unicamente in formato testo.

Quando si salvano file di grosse dimensioni, è possibile fare clic sul pulsante **Cancel** a fianco della barra di avanzamento per interrompere l'operazione di salvataggio.



In questo caso, il visualizzatore mostrerà solamente i dati ricevuti prima dell'interruzione del salvataggio.

Per salvare i dati visualizzati in un file esterno, fare clic sul pulsante **Save**.

Comando "External Viewer"
È possibile specificare un programma esterno per visualizzare le copie shadow dei dati. Una volta definita l'applicazione, il comando **External Viewer** diventa disponibile nel menu contestuale. Per specificare l'applicazione, aprire l'editor del Registro di sistema e inserire le seguenti informazioni sul computer su cui DeviceLock Management Console è in esecuzione:

- Chiave: **HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager**
- Nome: **ExternalShadowViewer**
- Tipo: **REG_SZ**
- Valore: *<percorso_completo_del_visualizzatore>* **%1**

  sostituire *<percorso_completo_del_visualizzatore>* con il percorso completo dell'applicazione esterna. Se il percorso include degli spazi, è necessario utilizzare i doppi apici. Ad esempio: "C:\Programmi\Microsoft Office\OFFICE11\winword.exe" %1.

  Quando si apre un file di grandi dimensioni, è possibile fare clic sul pulsante **Cancel** a fianco della barra di avanzamento per interrompere il processo di apertura. In tal caso, l'applicazione esterna aprirà solamente la parte dei dati ricevuti prima dell'interruzione dell'apertura.

Comando "Delete"
Per eliminare una voce in elenco, scegliere **Delete** dal menu contestuale oppure fare clic sul relativo pulsante sulla barra degli strumenti. Per evidenziare ed eliminare contemporaneamente più voci, utilizzare i tasti Ctrl e/o Maiusc.

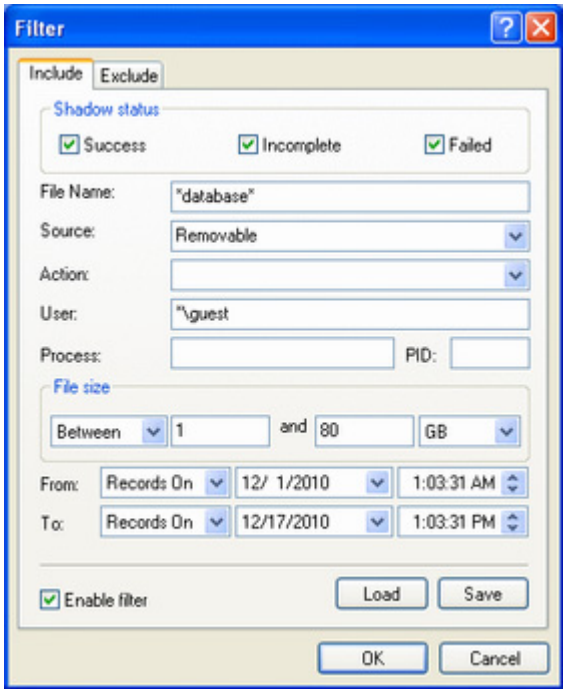
Comando "Refresh"
Per aggiornare il contenuto dell'elenco, selezionare **Refresh** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Comando "Send Data to Server"
Quando è necessario forzare lo spostamento delle copie shadow dei dati dal computer locale al server e DeviceLock Enterprise Server è stato specificato nelle impostazioni del servizio, scegliere **Send Data to Server** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante della barra degli strumenti.

Sezione Shadow Log Filter (Servizio)

È possibile filtrare i dati elencati nel visualizzatore degli eventi di shadowing in modo da elencare solamente le voci che corrispondono a determinati criteri.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic con il pulsante destro del mouse sulla barra degli strumenti.



Non esistono sostanziali differenze tra la definizione dei filtri degli eventi di controllo ed i filtri degli eventi di shadowing. Pertanto, si consiglia di leggere prima Sezione Audit Log Filter (Servizio).

Quando un filtro è attivo, è possibile definirne i criteri impostando i seguenti campi:

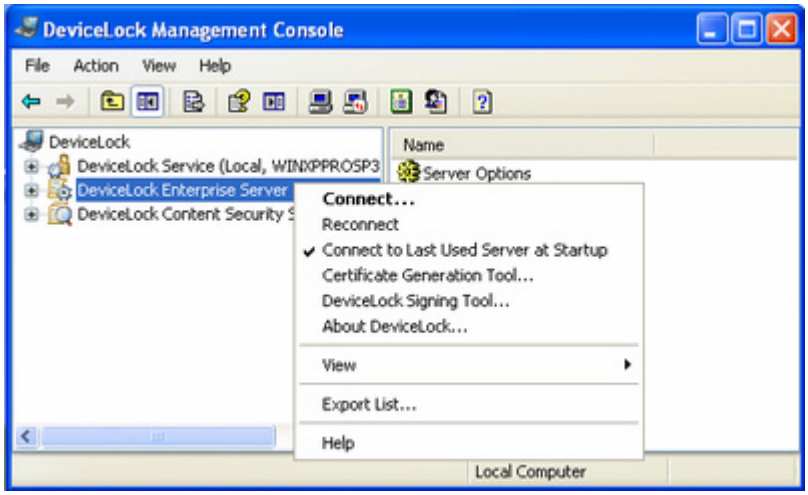
- **Success** – specifica se visualizzare i dati che sono stati correttamente registrati.
- **Incomplete** – specifica se visualizzare i dati che non sono stati completamente registrati.
- **Failed** - specifica se filtrare i dati registrati la cui trasmissione è stata bloccata dalle regole basate sul contenuto (Content-Aware Rules).
- **File Name** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **File Name** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Source** – casella in cui selezionare la voce che corrisponda a quella riportata nella colonna **Source** del visualizzatore di eventi.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Action** – casella in cui selezionare la voce che corrisponda a quella riportata nella colonna **Action** del visualizzatore di eventi.

È possibile inserire più valori separandoli con un punto e virgola (;).

- **User** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **User** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Process** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Process** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **PID** – casella in cui digitare un numero che corrisponda a quello riportato nella colonna **PID** del visualizzatore di eventi.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **File size** – valore o intervallo di valori che corrisponda a quello riportato nella colonna **File Size** del visualizzatore di eventi.
- **From** – specifica l'inizio dell'intervallo di eventi da filtrare. Selezionare **First Record** per visualizzare gli eventi a partire dal primo evento registrato. Selezionare **Records On** per visualizzare gli eventi che si sono verificati a partire da una data e da un'ora specifiche.
- **To** – specifica la fine dell'intervallo di eventi da filtrare. Selezionare **Last Record** per visualizzare gli eventi fino all'ultimo evento registrato. Selezionare **Records On** per visualizzare gli eventi che si sono verificati fino ad una data e ad un'ora specifiche.

Gestione di DeviceLock Enterprise Server

Espandere la sezione **DeviceLock Enterprise Server** per accedere alle funzioni e ai parametri di configurazione di un server.



È disponibile un menu contestuale richiamabile facendo clic con il pulsante destro del mouse sulla voce **DeviceLock Enterprise Server**:

- **Connect** – effettua la connessione al computer specificato. Per ulteriori informazioni, leggere la sezione Connessione ai computer.

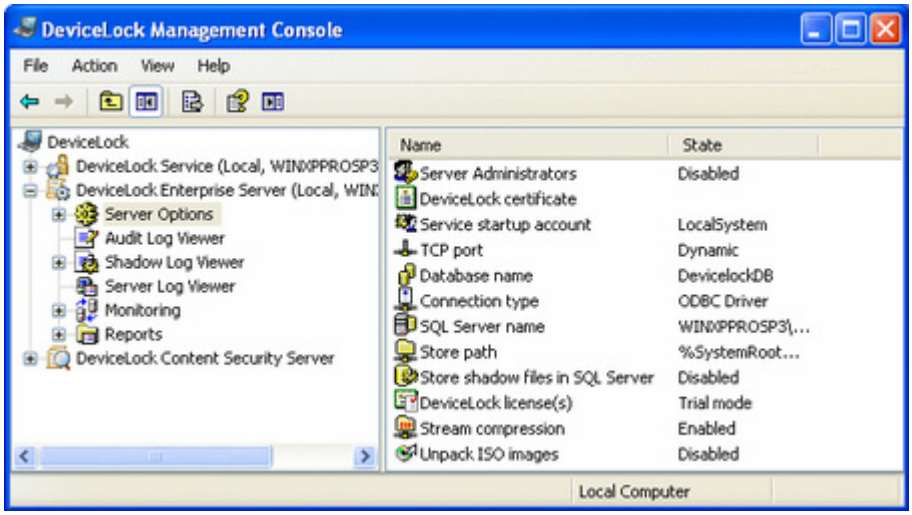
  Quando ci si connette ad un computer su cui è installata una versione meno recente di DeviceLock Enterprise Server, è possibile ricevere il seguente messaggio.

  In tal caso, è necessario installare su questo computer una nuova versione di DeviceLock Enterprise Server. Per ulteriori informazioni su come installare DeviceLock Enterprise Server, leggere la sezione Installazione di DeviceLock Enterprise Server.

- **Reconnect** – effettua nuovamente la connessione al computer al quale si è già connessi.
- **Connect to Last Used Server at Startup** – se si seleziona questa opzione, ad ogni avvio, DeviceLock Management Console si connette automaticamente all'ultimo server utilizzato.
- **Certificate Generation Tool** – avvia uno strumento speciale che consente di creare i certificati di DeviceLock. Per ulteriori informazioni, leggere la sezione Creazione dei certificati di DeviceLock.
- **DeviceLock Signing Tool** – avvia uno strumento speciale che consente agli utenti di accedere temporaneamente alle periferiche richieste e di firmare i file XML in cui sono incluse le impostazioni di DeviceLock Service. Per ulteriori informazioni, leggere la sezione relativa allo strumento DeviceLock Signing.
- **About DeviceLock** – mostra una finestra di dialogo e visualizza informazioni sul numero della versione di DeviceLock e sulla licenza.

Sezione Server Options (Server)

In questa sezione è possibile configurare le impostazioni di DeviceLock Enterprise Server.



Utilizzare il menu contestuale visualizzato facendo clic con il pulsante destro del mouse o fare doppio clic sul parametro **Stream compression** per attivarlo o disattivarlo. Se si attiva il parametro **Stream compression** DeviceLock comprime i registri di controllo e i dati di shadowing inviati dagli agenti DeviceLock Service a DeviceLock Enterprise Server. Ciò consente di diminuire le dimensioni dei trasferimenti di dati e di ridurre quindi il carico della rete.

Attivando il parametro **Unpack ISO images**, è possibile indicare a DeviceLock Enterprise Server di estrarre i file dalle immagini CD/DVD di shadowing. Se questo parametro è attivato, tutti i file vengono estratti dalle immagini CD/DVD al momento della consegna al server e memorizzati nel database separatamente (un record per file). In caso contrario, nel database vengono memorizzate le intere immagini CD/DVD di shadowing.

Utilizzare il menu contestuale disponibile per gli altri parametri per aprire le finestre di dialogo che consentono di apportare modifiche. In alternativa, è possibile fare doppio clic su un determinato parametro per aprire la finestra di dialogo corrispondente.

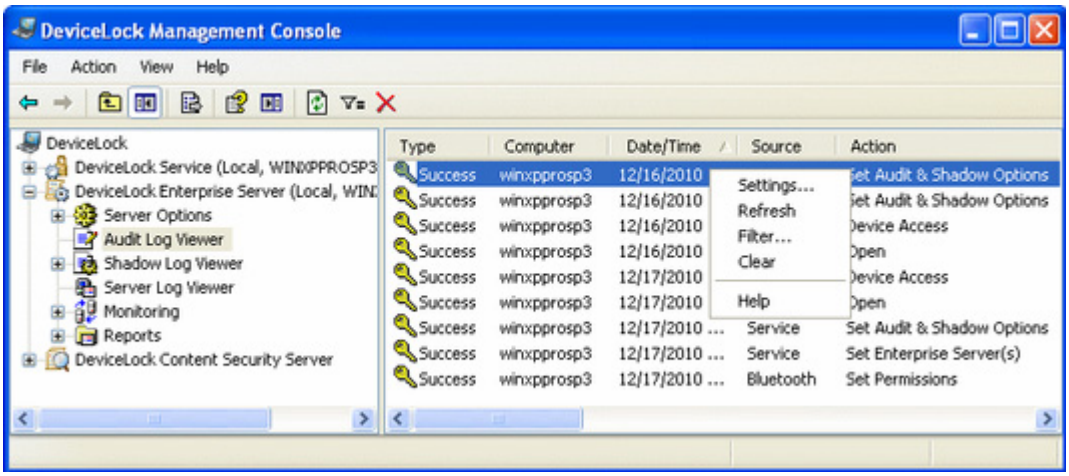
Tutti questi parametri sono descritti in dettaglio nella sezione Installazione di DeviceLock Enterprise Server.

Per avviare la procedura di configurazione guidata e modificare o impostare i parametri di DeviceLock Enterprise Server, scegliere **Properties** dal menu sensibile al contesto delle opzioni del server. Per informazioni sulla procedura guidata, leggere la sezione Installazione di DeviceLock Enterprise Server.

Sezione Audit Log Viewer (Server)

Utilizzando il visualizzatore di eventi è possibile visualizzare gli eventi di controllo memorizzati su DeviceLock Enterprise Server.

DeviceLock Enterprise Server memorizza gli eventi di controllo ricevuti da un computer remoto solamente se l'opzione **DeviceLock Log** oppure **Event & DeviceLock Logs** è selezionata nelle impostazioni del servizio di quel computer. Altrimenti, gli eventi di controllo vengono memorizzati utilizzando il sottosistema standard di registrazione degli eventi di Windows del computer remoto e possono essere visualizzati con il visualizzatore degli eventi del server.



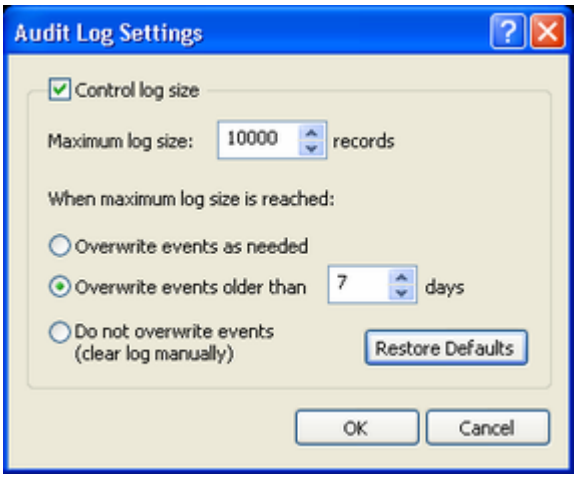
Non esistono sostanziali differenze tra il visualizzatore degli eventi di controllo del servizio e il visualizzatore degli eventi di controllo del server. Pertanto, si consiglia di leggere Sezione Audit Log Viewer (Servizio).

Rispetto al visualizzatore del registro di controllo del servizio, il visualizzatore del server presenta le seguenti colonne aggiuntive:

- **Computer** – il nome del computer da cui sono stati ricevuti gli eventi di controllo.
- **Event** – un numero che identifica il particolare tipo di evento.
- **Received Date/Time** – data e ora in cui un evento è stato ricevuto da DeviceLock Enterprise Server.

Sezione Audit Log Settings (Server)

Per definire la dimensione massima del file registro e specificare l'operazione che DeviceLock Enterprise Server deve eseguire quando il registro diventa pieno, selezionare **Settings** dal menu contestuale richiamabile con il pulsante destro del mouse.



Nota: queste impostazioni sono memorizzate nel database e sono specifiche del file registro, ma non di DeviceLock Enterprise Server. Ciò significa che, se più server di DeviceLock Enterprise utilizzano un unico database, questi utilizzano tutti le stesse impostazioni del file registro.

Se si seleziona la casella di controllo Control log size, DeviceLock Enterprise Server controllerà il numero di voci presenti nel registro e, se necessario, eliminerà le voci meno recenti, in modo da recuperare spazio e consentire la memorizzazione di nuovi record. Se la casella di controllo **Control log size** è deselezionata, DeviceLock Enterprise Server memorizzerà gli eventi utilizzando tutto lo spazio disponibile del database SQL Server.

Il parametro **Maximum log size** specifica il numero massimo di record che questo file registro può contenere. Se più server di DeviceLock Enterprise utilizzano questo database, il numero corrente di record memorizzati nel file registro può essere maggiore (di due record) rispetto al valore specificato.

Per specificare l'operazione che deve eseguire DeviceLock Enterprise Server quando il file registro diventa pieno (ovvero, quando la dimensione del registro corrisponde al valore assegnato al parametro Maximum log size), selezionare una delle seguenti opzioni:

- **Overwrite events as needed** – il server sostituisce gli eventi meno recenti con quelli più recenti quando il registro è pieno, ovvero quando la dimensione del file registro corrisponde al valore assegnato al parametro **Maximum log size**.
- **Overwrite events older than** – specifica il numero di giorni in cui il file registro verrà mantenuto prima di essere sovrascritto.
- **Do not overwrite events (clear log manually)** – gli eventi esistenti verranno mantenuti quando il registro è pieno, ovvero quando la dimensione del file registro corrisponde al valore assegnato al parametro **Maximum log size**. È necessario cancellare manualmente il contenuto del file registro.

Per reimpostare i valori predefiniti delle impostazioni, fare clic sul pulsante **Restore Defaults**. I valori predefiniti sono i seguenti:

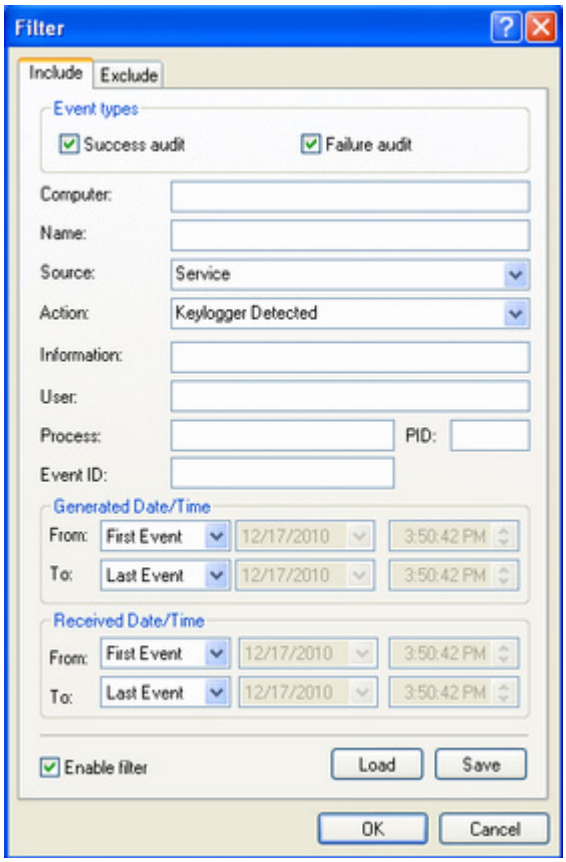
- il valore predefinito del parametro **The Maximum log size** è 10000 record.
- l'operazione predefinita è **Overwrite events older than** e il numero di giorni predefinito è 7.

Se lo spazio disponibile nel file registro non è sufficiente per accogliere nuovi record e non esistono informazioni che possono essere eliminate, DeviceLock Enterprise Server non rimuoverà gli eventi di controllo dai computer remoti degli utenti. Questo impedisce la perdita dei dati dovuta alla mancanza di spazio nel file registro. Non appena lo spazio diventa disponibile, DeviceLock Enterprise Server sposta gli eventi di controllo rimanenti dai computer degli utenti al file registro.

Sezione Audit Log Filter (Server)

È possibile filtrare i dati visualizzati nel visualizzatore degli eventi di controllo in base a determinati criteri.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.



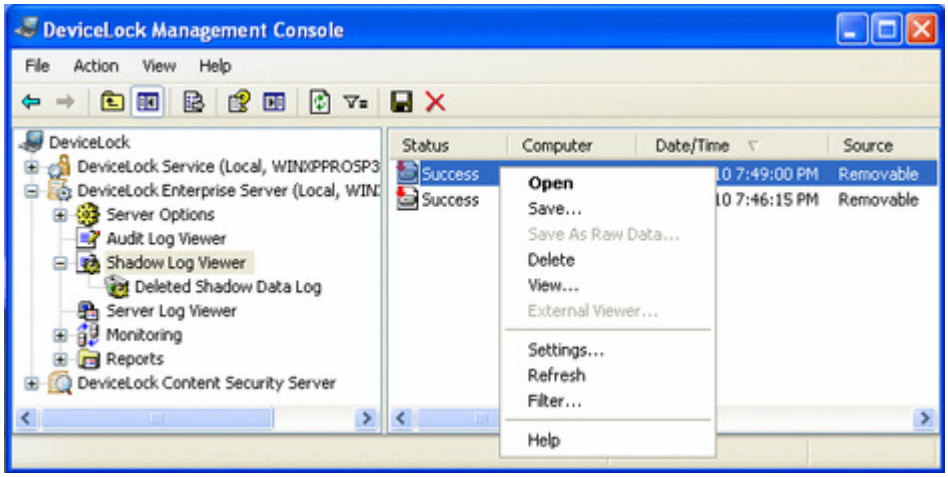
Non esistono sostanziali differenze tra i filtri degli eventi di controllo del servizio ed i filtri degli eventi di controllo del server. Pertanto, si consiglia prima di leggere Sezione Audit Log Filter (Servizio).

Rispetto al filtro del registro di controllo del servizio, il filtro del server presenta i seguenti campi aggiuntivi:

- **Computer** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Computer** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly. *È possibile inserire più valori separandoli con un punto e virgola (;).*
- **Event ID** – casella in cui digitare un numero che corrisponda a quello riportato nella colonna **Event** del visualizzatore di eventi. *È possibile inserire più valori separandoli con un punto e virgola (;).*
- **Received Date/Time** - specifica il periodo di tempo utilizzato per filtrare gli eventi in base a quando sono stati ricevuti da DeviceLock Enterprise Server. **From:** indica la data e l'ora iniziali degli eventi da visualizzare, mentre **To:** specifica la data e l'ora finali degli eventi da visualizzare. I valori possibili per il parametro **From:** sono **First Event** ed **Events On**. Selezionare **First Event** per visualizzare gli eventi a partire dal primo evento ricevuto da DeviceLock Enterprise Server. Selezionare **Events On** per visualizzare gli eventi ricevuti che iniziano in una data e un'ora specifiche. I valori possibili per il parametro **To:** sono **Last Event** ed **Events On**. Selezionare **Last Event** per visualizzare gli eventi fino all'ultimo evento ricevuto da DeviceLock Enterprise Server. Selezionare **Events On** per visualizzare gli eventi ricevuti e che terminano in una data e un'ora specifiche.

Sezione Shadow Log Viewer (Server)

Il visualizzatore di eventi di shadowing consente di visualizzare gli eventi di shadowing memorizzati su DeviceLock Enterprise Server.



Non esistono sostanziali differenze tra il visualizzatore degli eventi di shadowing del servizio e il visualizzatore degli eventi di shadowing del server. Pertanto, si consiglia prima di leggere Sezione Shadow Log Viewer (Servizio).

Rispetto al visualizzatore del registro shadow del servizio, il visualizzatore del server presenta due colonne aggiuntive:

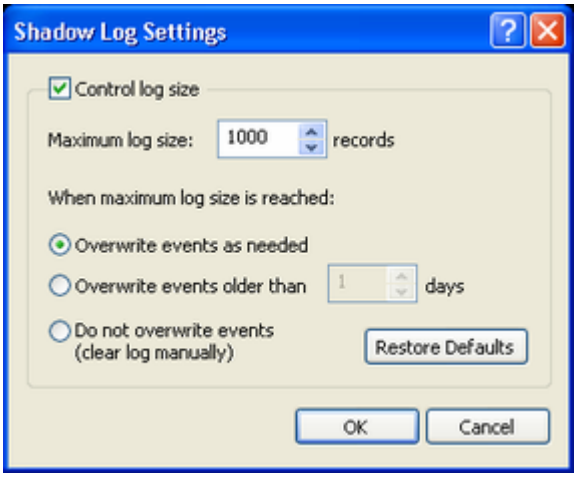
- **Computer** – il nome del computer da cui sono stati ricevuti gli eventi di shadowing.
- **Received Date/Time** – data e ora in cui un record è stato ricevuto da DeviceLock Enterprise Server.

A differenza del visualizzatore degli eventi di shadowing del servizio, quando viene eliminato un record, i dati binari del record vengono rimossi dal database o dal disco (in base allo stato dell'opzione Store shadow files in SQL Server), mentre tutte le altre informazioni (quali il nome del file e la dimensione, il nome dell'utente, la data e l'ora, il processo e così via) vengono spostate in un file registro speciale chiamato Deleted Shadow Data Log.

Questo registro speciale viene utilizzato quando è necessario conservare le informazioni sui dati trasferiti ma il contenuto delle copie shadow dei dati non è più necessario e si desidera pulire l'area di archiviazione (il database di SQL Server o il disco).

Sezione Shadow Log Settings

Per definire la dimensione massima del file registro e specificare l'operazione che DeviceLock Enterprise Server deve eseguire quando il registro degli eventi di shadowing diventa pieno, selezionare **Settings** dal menu contestuale richiamabile con il pulsante destro del mouse.



Per informazioni sulle impostazioni, leggere Sezione Audit Log Settings (Server).

Quando DeviceLock Enterprise Server deve rimuovere i record più vecchi dal registro degli eventi di shadowing (in base alla configurazione dei parametri **Overwrite events as needed** e **Overwrite events older than**), sposta tali record nel registro speciale Deleted Shadow Data Log.

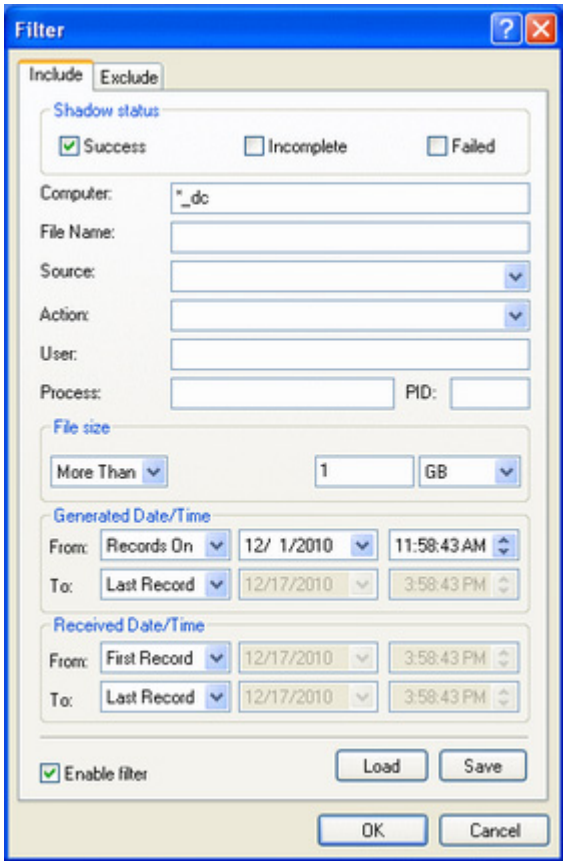
Se lo spazio disponibile nel file registro non è sufficiente per accogliere nuovi record e non esistono informazioni che possono essere eliminate, DeviceLock Enterprise Server non rimuoverà i dati di shadowing dai computer remoti degli utenti. Questo impedisce la perdita dei dati dovuta alla mancanza di spazio nel registro eventi. Non appena lo spazio diventa disponibile, DeviceLock Enterprise Server sposta gli eventi di shadowing rimanenti dai computer degli utenti al file registro.

È meglio evitare di accumulare copie shadow dei dati sui computer degli utenti. Si raccomanda di monitorare il file registro di DeviceLock Enterprise Server su base periodica, in modo da leggere i messaggi di avvertimento e modificare le impostazioni in modo appropriato.

Sezione Shadow Log Filter (Server)

È possibile filtrare i dati visualizzati nel visualizzatore degli eventi di shadowing in base a determinati criteri.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.



Non esistono sostanziali differenze tra i filtri degli eventi di shadowing del servizio ed i filtri degli eventi di shadowing del server. Pertanto, si consiglia prima di leggere Sezione Shadow Log Filter (Servizio).

Rispetto al filtro del registro shadow del servizio, il filtro del server presenta i seguenti campi aggiuntivi:

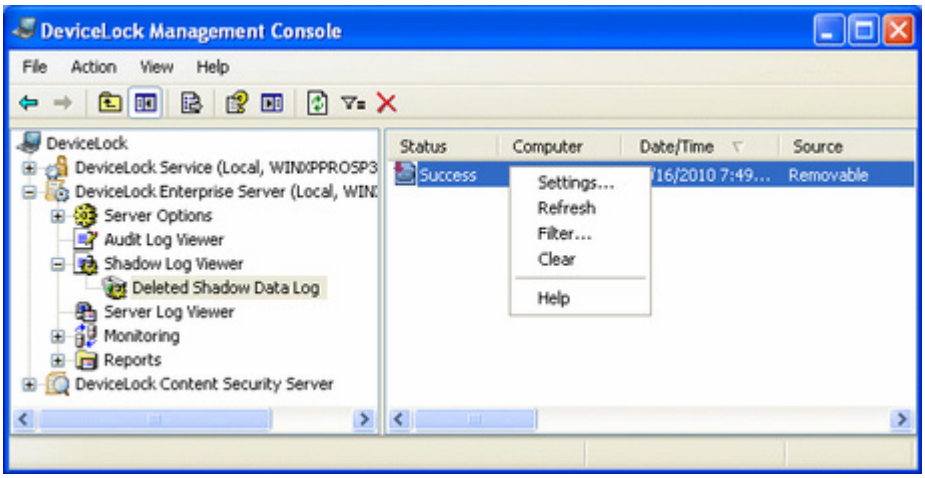
- **Computer** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Computer** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly. *È possibile inserire più valori separandoli con un punto e virgola (;).*
- **Received Date/Time** - specifica il periodo di tempo utilizzato per filtrare i record in base a quando sono stati ricevuti da DeviceLock Enterprise Server. **From:** indica la data e l'ora iniziali dei record da visualizzare, mentre **To:** specifica la data e l'ora finali dei record da visualizzare. I valori possibili per il parametro **From:** sono **First Record** e **Records On**. Selezionare **First Record** per visualizzare i record a partire dal primo record ricevuto da DeviceLock Enterprise Server. Selezionare **Records On** per visualizzare i record ricevuti a partire da una data e un'ora specifiche. I valori possibili per il parametro **To:** sono **Last Record** ed **Records On**. Selezionare **Last Record** per visualizzare i record fino all'ultimo record ricevuto da DeviceLock Enterprise Server. Selezionare **Records On** per visualizzare i record ricevuti

fino a una data e un'ora specifiche.

Sezione Deleted Shadow Data Log

Questo visualizzatore consente di ottenere informazioni sui record dei registri eventi di shadowing eliminati.

Quando un record viene eliminato dal visualizzatore degli eventi di shadowing, i dati binari del record vengono rimossi, mentre tutte le altre informazioni (quali il nome del file e la dimensione, il nome dell'utente, la data e l'ora, il processo e così via) vengono spostate in questo file registro.



Questo registro speciale viene utilizzato quando è necessario conservare le informazioni sui dati trasferiti, ma il contenuto delle copie shadow dei dati non è più necessario e si desidera pulire l'area di archiviazione (il database di SQL Server o il disco).

Per definire la dimensione massima del file registro e specificare l'operazione che DeviceLock Enterprise Server deve eseguire quando il registro degli eventi di shadowing diventa pieno, selezionare **Settings** dal menu contestuale richiamabile con il pulsante destro del mouse. Le impostazioni di questo registro sono simili a quelle del registro di controllo. Pertanto, si consiglia prima di leggere Sezione Audit Log Settings (Server).

Se lo spazio disponibile nel file registro non è sufficiente per accogliere nuovi record e non esistono voci che possono essere eliminate, DeviceLock Enterprise Server ignorerà l'aggiunta di nuovi record. Per evitare la perdita dei record, si consiglia di monitorare il file registro di DeviceLock Enterprise Server su base periodica e di prestare attenzione alla presenza di eventuali messaggi di avvertimento.

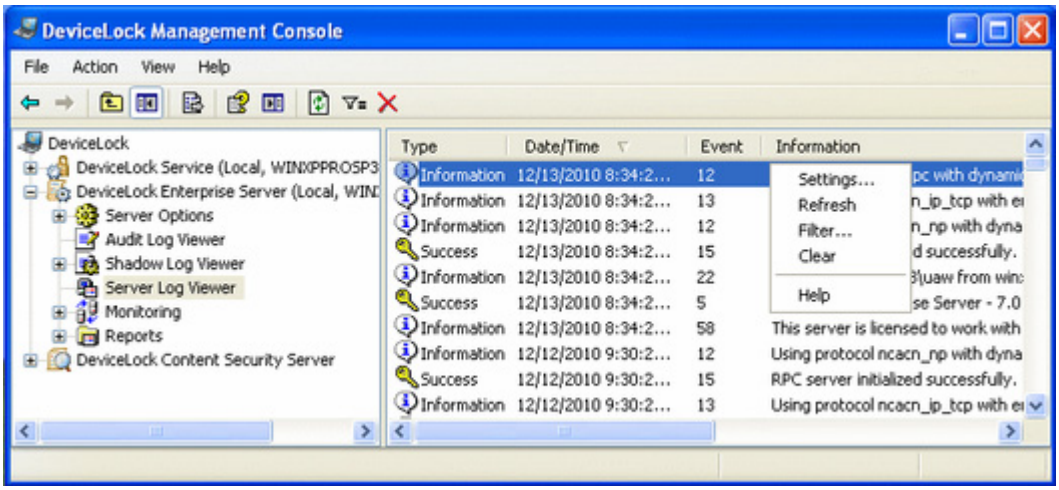
Per aggiornare il registro eventi, selezionare **Refresh** dal menu contestuale richiamabile con il pulsante destro del mouse oppure facendo clic sul relativo pulsante sulla barra degli strumenti.

Per filtrare i record in elenco, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti. Poiché il visualizzatore degli eventi di shadowing utilizza lo stesso tipo di filtro, si consiglia di leggere Sezione Shadow Log Filter (Server).

Per cancellare il contenuto del registro, selezionare **Clear** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.

Sezione Server Log Viewer

Questo visualizzatore consente di visualizzare il registro eventi interno di DeviceLock Enterprise Server. Il server memorizza in questo registro gli eventi relativi agli errori di scrittura, i messaggi di avvertimento ed altre importanti informazioni (quali le modifiche apportate alla configurazione, gli eventi di avvio/arresto, il numero di versione ed altro ancora).



I dati contenuti in questo registro possono essere utilizzati per diagnosticare eventuali problemi, per monitorare le modifiche apportate alla configurazione del server e per ottenere informazioni su chi ha reimpostato i file registro e quando.

Il visualizzatore di eventi mostra le seguenti informazioni:

- **Type** – la classe di un evento. Può assumere i seguenti valori: **Success**, **Information**, **Warning** oppure **Error**.
- **Date/Time** – la data e l'ora in cui si è verificato l'evento.
- **Event** – un numero che identifica il particolare tipo di evento.
- **Information** – informazioni specifiche sull'evento, quali la descrizione dei messaggi di avvertimento e/o di errore, i nomi ed i valori dei parametri modificati e così via.
- **Server** – il nome del server su cui si è verificato l'evento.

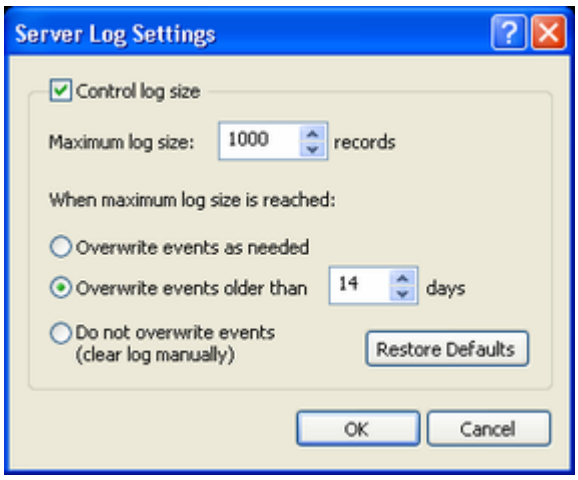
- **Record N** – il numero del record.

Per aggiornare il registro eventi, selezionare **Refresh** dal menu contestuale richiamabile con il pulsante destro del mouse oppure facendo clic sul relativo pulsante sulla barra degli strumenti. Per cancellare il contenuto del registro, selezionare **Clear** dal menu contestuale richiamabile con il pulsante destro del mouse oppure facendo clic sul relativo pulsante sulla barra degli strumenti.

Una volta cancellati tutti gli eventi, nel registro viene scritto un evento relativo all'operazione di cancellazione (ad esempio: "The Server Log (100 record(s)) was cleared by VM2000AD\Administrator from xpvirt.vm2000ad.com").

Sezione Server Log Settings

Per definire la dimensione massima del file registro e specificare l'operazione che DeviceLock Enterprise Server deve eseguire quando il registro degli eventi diventa pieno, selezionare **Settings** dal menu contestuale richiamabile con il pulsante destro del mouse.



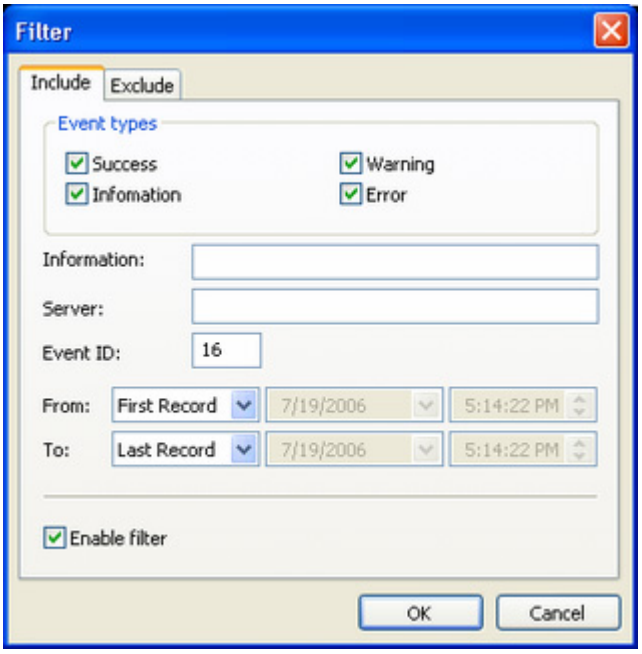
Per informazioni sulle impostazioni, leggere Sezione Audit Log Settings (Server).

Se lo spazio disponibile nel file registro di shadowing non è sufficiente per accogliere nuovi record e non esistono voci che possono essere eliminate, DeviceLock Enterprise Server non aggiungerà i nuovi record.

Sezione Server Log Filter

È possibile filtrare i dati visualizzati nel visualizzatore degli eventi del server in base a determinati criteri.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale richiamabile con il pulsante destro del mouse oppure fare clic sul relativo pulsante sulla barra degli strumenti.



Non esistono sostanziali differenze tra i filtri degli eventi di controllo del servizio ed i filtri degli eventi di controllo del server. Pertanto, si consiglia prima di leggere Sezione Audit Log Filter (Servizio).

Quando un filtro è attivato, è possibile definirne i criteri impostando i seguenti campi:

- **Success** – specifica se filtrare gli eventi della classe **Success**.
- **Information** – specifica se filtrare gli eventi della classe **Information**.
- **Warning** – specifica se filtrare gli eventi della classe **Warning**.
- **Error** – specifica se filtrare gli eventi della classe **Error**.
- **Information** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Information** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Server** – casella in cui digitare testo che corrisponda a quello riportato nella colonna **Server** del visualizzatore di eventi. Questo campo non fa distinzione tra maiuscole e minuscole ed è possibile utilizzare i caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Event ID** – casella in cui digitare un numero che corrisponda a quello riportato nella colonna **Event** del visualizzatore di eventi.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **From** – specifica l'inizio dell'intervallo di eventi da filtrare. Selezionare **First Event** per visualizzare gli eventi a partire dal primo evento registrato. Selezionare **Events On** per visualizzare gli eventi che si sono verificati a partire da una data e da un'ora specifiche.

- **To** – specifica la fine dell'intervallo di eventi da filtrare. Selezionare **Last Event** per visualizzare gli eventi fino all'ultimo evento registrato. Selezionare **Events On** per visualizzare gli eventi che si sono verificati fino ad una data e ad un'ora specifiche.

Monitoraggio

Questa funzionalità di DeviceLock Enterprise Server consente di implementare il monitoraggio in tempo reale dei DeviceLock Service all'interno della rete. DeviceLock Enterprise Server è in grado di monitorare i computer remoti in tempo reale, verificando lo stato di DeviceLock Service (attivo o meno) e l'uniformità e l'integrità dei criteri. Le informazioni dettagliate vengono inserite in un apposito registro di monitoraggio e possono essere visualizzate utilizzando Monitoring Log Viewer.

È inoltre possibile definire una serie di criteri principali da applicare automaticamente in tutti i computer remoti, se si sospetta che in questi ultimi i criteri siano obsoleti o danneggiati.

Infine, è possibile utilizzare questa funzionalità di ripristino dei criteri come metodo alternativo per implementare impostazioni, autorizzazioni, controlli e regole di shadowing nei DeviceLock Service remoti all'interno della rete.

Panoramica dell'architettura

Tutte le azioni (monitoraggio dei computer, verifica dell'uniformità e dell'integrità dei criteri, ecc.) vengono eseguite dalle attività.

È possibile disporre di tutte le attività desiderate su un singolo DeviceLock Enterprise Server. Il numero massimo di attività incluse in un server, infatti, dipende unicamente dalla memoria disponibile, dalle caratteristiche della CPU e dalla larghezza di banda della rete. Si noti che il server deve disporre di risorse sufficienti per comunicare con almeno 10 computer remoti contemporaneamente.

Per impostazione predefinita, DeviceLock Enterprise Server può eseguire un massimo di 30 attività simultaneamente. Ciò significa che, in presenza di 40 attività eseguite simultaneamente, vengono inizialmente effettuate le prime 30, mentre ognuna delle 10 restanti si avvia una volta terminate le precedenti.

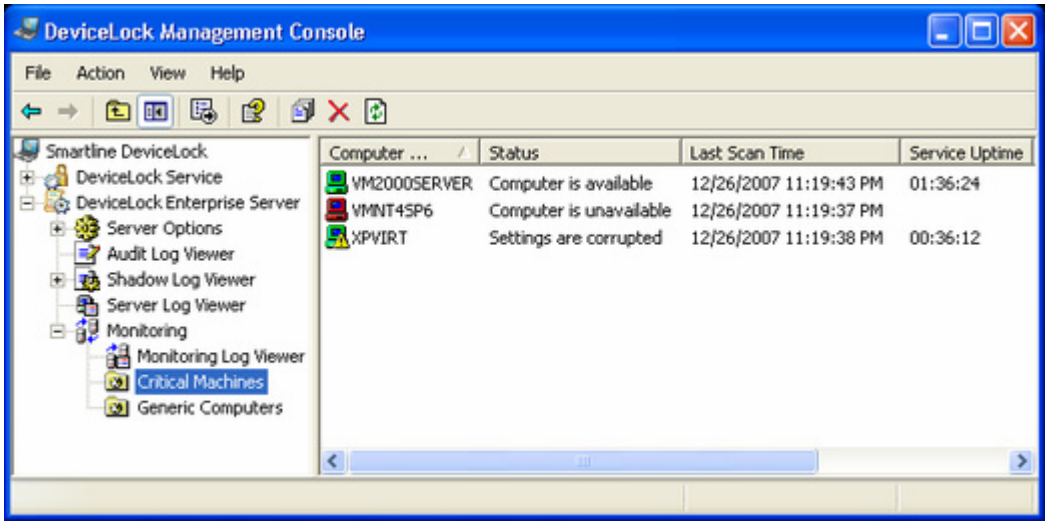
Tuttavia, è possibile modificare il numero di attività da eseguire simultaneamente modificando alcuni valori nel registro. Per definire un nuovo numero, aprire **Regedit** e impostare quanto segue sul computer in cui è in esecuzione DeviceLock Enterprise Server:

- Chiave: **HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer**
- Nome: **ConcurrentJobs**

- Tipo: **DWORD**
- Valore: *numero_di_thread*
  in cui *numero_di_thread* deve essere un valore compreso tra 1 e 1000.

Durante l'esecuzione, le attività scrivono le informazioni sullo stato nel registro di monitoraggio, tra cui i dati sui computer monitorati e sui DeviceLock Service. Le attività, inoltre, registrano eventuali errori che si verificano durante l'analisi dei computer e la connessione ai DeviceLock Service.

Infine, le attività mostrano lo stato dei computer monitorati e altre informazioni utili alla console di gestione. Tutti ciò permette di verificare lo stato dei computer monitorati in tempo reale.



Per visualizzare i computer monitorati che appartengono all'attività, selezionarla nella struttura a sinistra.

Per aggiornare le informazioni visualizzate nell'elenco dei computer, selezionare Refresh dal menu contestuale che compare facendo clic con il pulsante destro del mouse o premendo l'apposito pulsante nella barra degli strumenti.

- **Computer Name** – nome del computer monitorato.
- **Status** – stato del computer monitorato e di DeviceLock Service.
  Lo stato influenza anche l'icona posta accanto al parametro **Computer Name**. Regole generali di interpretazione delle icone del computer:
  - Computer verde – il computer è in attività e DeviceLock Service è in esecuzione sullo stesso.
  - Computer rosso – il computer non è in attività/non è stato trovato o è in attività ma senza DeviceLock Service.
  - Computer con punto esclamativo – Presenza di problemi nel computer o in DeviceLock Service.

  Gli stati sono otto:

1. **Computer is available** – il computer monitorato è in attività e DeviceLock Service è in esecuzione sullo stesso. Inoltre, se questa attività verifica l'integrità dei criteri, la verifica non ha trovato alcun errore. L'icona è il "computer verde".

   Se questa attività ripristina il criterio infranto, l'icona visualizzata è un computer verde con il punto esclamativo.

2. **Computer is unavailable** – DeviceLock Enterprise Server non può analizzare il computer monitorato. Ciò si verifica quando un computer non è in attività o le connessioni sono bloccate da un firewall, ma il nome/l'indirizzo del computer può essere risolto tramite DNS. L'icona è il "computer rosso".
3. **Service is unavailable** – DeviceLock Enterprise Server non è grado di collegarsi a DeviceLock Service sul computer monitorato. Ciò si verifica quando il computer è in attività ma DeviceLock Service non è in esecuzione. Può essere inoltre il risultato di DeviceLock Service in esecuzione su una porta TCP diversa da quella specificata nella configurazione dell'attività o di connessioni bloccate dal firewall. L'icona è il "computer rosso con punto esclamativo". Per ulteriori informazioni sui problemi di connessione, leggere la descrizione del parametro Service connection settings.
4. **Settings are corrupted** – il computer monitorato è in attività e DeviceLock Service è in esecuzione sul computer, ma il processo di verifica dei criteri non è andato a buon fine. Ciò si verifica se i criteri principali vengono assegnati a un'attività e non corrispondono ai criteri del DeviceLock Service monitorato. L'icona è il "computer verde con punto esclamativo".
5. **Unresolved computer address** – DeviceLock Enterprise Server non è in grado di risolvere il nome/l'indirizzo del computer. Ciò si verifica quando viene specificato un nome di computer non valido che non esiste nel DNS, o se non è presente alcun server DNS. Nel secondo caso, lo stato **Unresolved computer address** viene trattato come **Computer is unavailable**. L'icona è il "computer rosso con punto esclamativo".
6. **Unsupported service version** – DeviceLock Enterprise Server sta tentando di scaricare una serie di criteri (impostazioni servizio) da DeviceLock Service versione 6.2 o inferiore. La verifica dei criteri è supportata solo per le versioni 6.2.1 e successive. L'icona è il "computer verde con punto esclamativo".
7. **Access is denied** – DeviceLock Enterprise Server non è grado di collegarsi a DeviceLock Service a causa di privilegi insufficienti. Ciò si verifica quando l'account con cui viene avviato il servizio DeviceLock Enterprise Server non possiede i diritti di connessione a DeviceLock Service. L'icona è il "computer verde con punto esclamativo". Per ulteriori informazioni su come risolvere il problema, leggere la descrizione del parametro Service connection settings.
8. **No License** – questo stato indica che DeviceLock Enterprise Server non può monitorare il computer che esegue DeviceLock Service a causa del numero insufficiente di licenze. DeviceLock Enterprise Server gestisce un numero di istanze DeviceLock Service pari al numero di licenze caricate nel DeviceLock Enterprise Server. Per maggiori informazioni, consultare la sezione "License information" in

"Installazione di DeviceLock Enterprise Server". L'icona del computer mostra un "computer verde con punto esclamativo".

Inoltre, gli stessi messaggi di stato (tranne **Computer is available**) vengono inseriti nel registro di monitoraggio, consentendo agli utenti di verificare la situazione dei computer monitorati in un secondo momento.

- **Last Scan Time** – data e ora dell'ultimo tentativo di scansione, indipendentemente dalla sua riuscita.
- **Last Successful Scan Time** – data e ora dell'ultimo tentativo di scansione eseguito correttamente.
- **Service Uptime** – mostra per quanto tempo DeviceLock Service ha lavorato sul computer monitorato.
- **Computer Uptime** – mostra per quanto tempo ha lavorato il computer monitorato. Confrontando il tempo di attività del computer con quello del servizio (vedere in alto), è possibile sapere se DeviceLock service è stato interrotto durante la sessione del computer corrente.
- **Service Version** – la versione di DeviceLock Service. Le ultime cinque cifre indicano il numero di build.

Algoritmo di monitoraggio

L'algoritmo utilizzato nel processo di monitoraggio è semplice ma efficace.

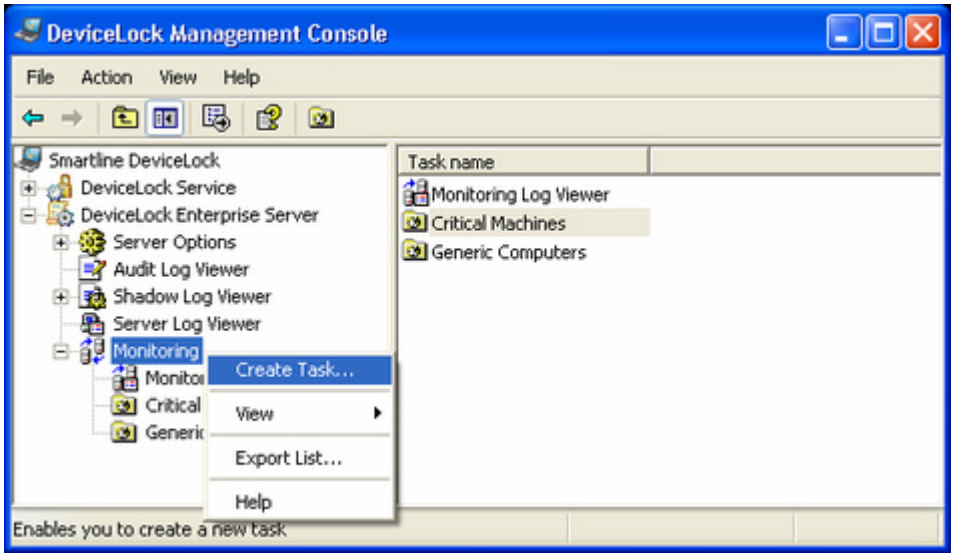
1. Inizialmente, DeviceLock Enterprise Server tenta di analizzare il computer monitorato per determinare se è in attività o meno. Se il risultato è positivo, il computer riceve lo stato **available** e il monitoraggio prosegue. In caso contrario, riceve lo stato **unavailable** e il monitoraggio termina (il record viene inserito nel registro di monitoraggio).
2. Successivamente, DeviceLock Enterprise Server tenta di collegarsi a DeviceLock Service. Se la connessione viene eseguita correttamente, DeviceLock Service riceve lo stato **available** e il monitoraggio del computer prosegue. In caso contrario, riceve lo stato **unavailable** e il monitoraggio termina (il record viene inserito nel registro di monitoraggio).
3. Se l'attività deve verificare l'integrità dei criteri di DeviceLock Service, il monitoraggio del computer prosegue. In caso contrario, il monitoraggio del computer termina (nulla viene inserito nel registro).
4. DeviceLock Enterprise Server scarica i criteri da DeviceLock Service e li confronta con la serie di criteri principale assegnata all'attività. Se non viene rilevata alcuna differenza, il monitoraggio del computer termina (nulla viene inserito nel registro). Se vi sono differenze tra i criteri, il monitoraggio del computer prosegue (il record viene inserito nel registro di monitoraggio).
5. Se l'attività deve ripristinare il criterio infranto, DeviceLock Enterprise Server scrive la serie di criteri principale nel DeviceLock Service e il monitoraggio del computer termina (il record viene inserito nel registro di monitoraggio). In caso contrario, il monitoraggio del computer termina (nulla viene inserito nel registro).

In presenza di errori in uno qualsiasi dei passaggi descritti in precedenza, il relativo record viene inserito nel registro di monitoraggio. Se l'errore non è di tipo critico, il monitoraggio prosegue. Se l'errore è di tipo critico, il monitoraggio del computer termina.

La presenza di errori particolarmente critici (ad esempio "memoria insufficiente") può interrompere l'esecuzione dell'intera attività.

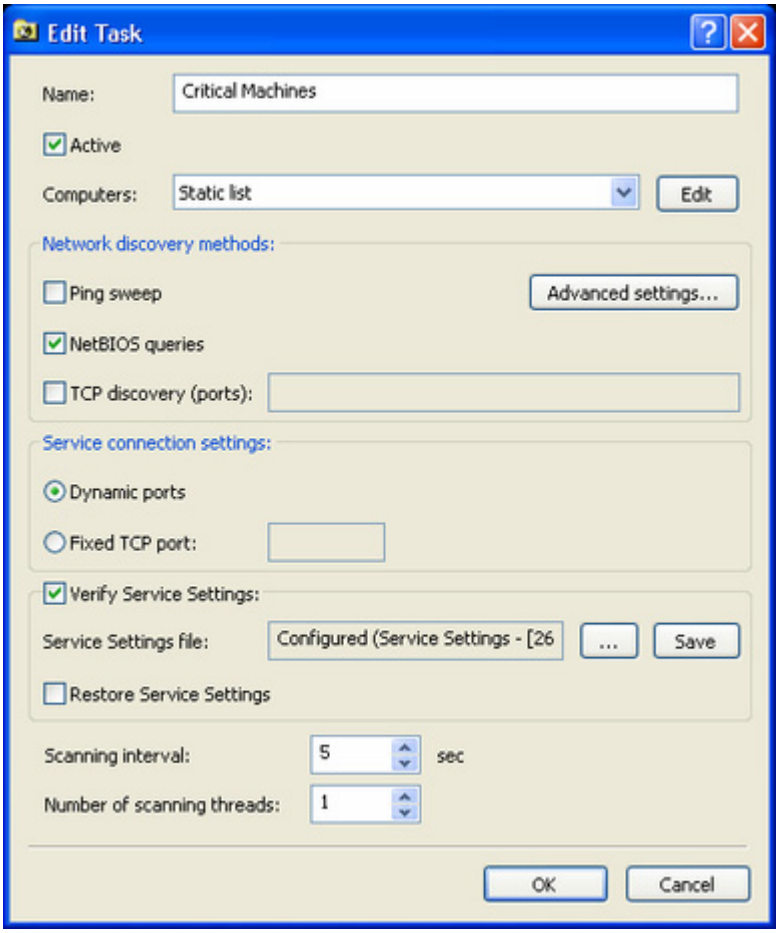
Creazione e modifica delle attività

Ciascuna attività include una serie di computer, azioni e parametri di configurazione.



Per creare una nuova attività, selezionare **Create Task** dal menu contestuale della voce **Monitoring** . Per modificare un'attività esistente, selezionarla nella struttura a sinistra e scegliere **Edit Task** dal menu contestuale.

Per eliminare definitivamente un'attività, selezionarla nella struttura a sinistra e scegliere **Delete Task** dal menu contestuale.



Name – nome dell'attività utilizzata per identificarla nell'elenco delle attività e nel registro di monitoraggio.

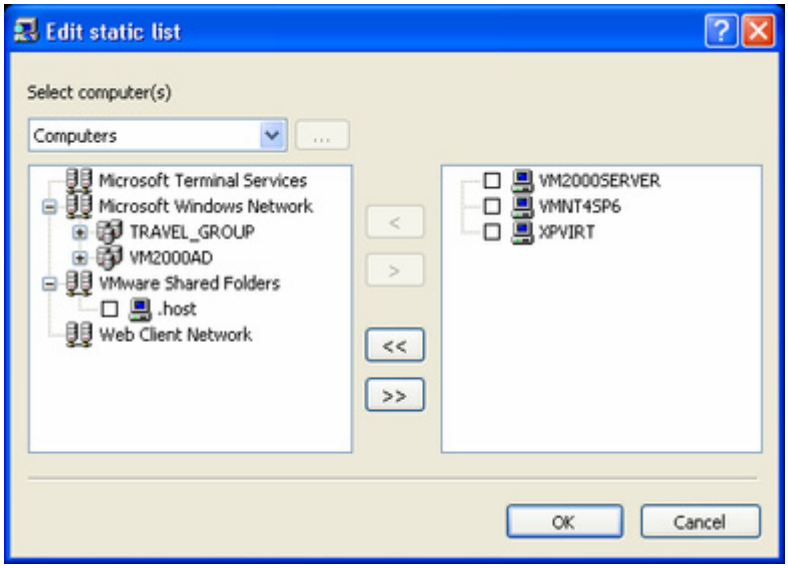
Active – se selezionato, consente a DeviceLock Enterprise Server di eseguire l'attività. Se si desidera disattivare l'attività senza eliminarla definitivamente, deselezionare questo flag.

Computers – il tipo di elenco di computer utilizzato per definire i computer che verranno monitorati dall'attività.

Premere il pulsante **Edit** per configurare l'elenco selezionato in **Computers**.

Sono supportati due tipi di elenco di computer:

1. **Static list** – tutti i computer vengono elencati in base al loro nome o indirizzo IP. Poiché si tratta di un elenco statico, anche se alcuni computer non sono più presenti nella rete, vengono monitorati (con registrazione degli errori) fino a quando il record non viene eliminato manualmente dall'elenco.



I computer da monitorare vanno specificati nell'elenco a destra. Selezionare i computer desiderati nell'elenco a sinistra, quindi spostarli nell'elenco a destra premendo il pulsante **>**.

Se occorre escludere alcuni computer dal processo di monitoraggio, selezionarli nell'elenco a destra e premere il pulsante **<**.

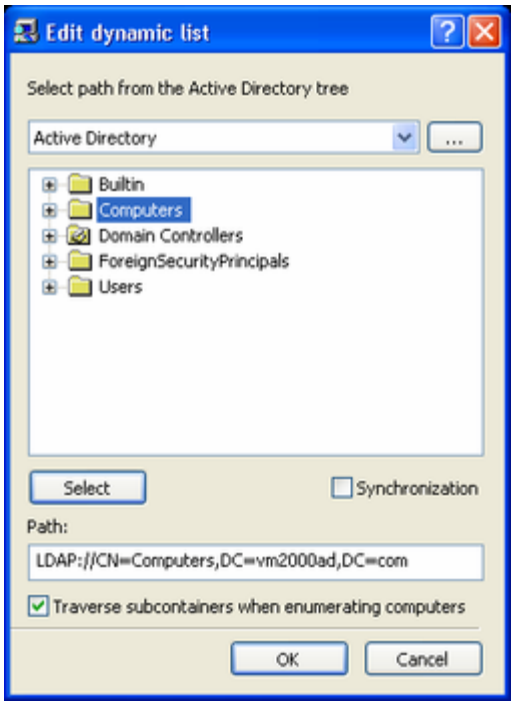
Utilizzando i pulsanti **>>** e **<<**, è possibile aggiungere e rimuovere tutti i computer disponibili simultaneamente (non è necessario selezionare i computer dall'elenco).

È possibile scegliere i computer della rete presenti nell'elenco a sinistra in diversi modi:

- **Computers** – sfogliare la struttura di rete e selezionare i computer.
- **From File** – caricare un elenco predefinito di computer dal file di testo esterno, quindi selezionare i computer. Per aprire un file esterno, premere il pulsante **...** . I file di testo devono includere il nome o l'indirizzo IP di ciascun computer su linee separate e possono essere di tipo Unicode o non Unicode.
- **Manual** – digitare i nomi di computer manualmente per selezionarli. Ciascun nome o indirizzo IP di computer deve essere inserito in una linea separata.

2. **Dynamic list** – al posto dei nomi o indirizzi IP dei computer, l'elenco dinamico include un percorso verso il contenitore (ad esempio unità organizzativa) nella struttura dei servizi di directory (ad esempio Active Directory, Novell eDirectory, OpenLDAP, ecc.) Ogni volta che l'attività viene eseguita, DeviceLock Enterprise Server recupera tutti i computer inclusi nel contenitore. Di conseguenza, se alcuni computer vengono rimossi dalla struttura delle directory o spostati in un altro contenitore, non vengono più monitorati. Viceversa, in presenza di nuovi computer che non erano inclusi nel contenitore al momento in cui l'attività è stata creata/modificata, e che sono stati aggiunti nel contenitore in seguito, vengono recuperati e monitorati al momento dell'esecuzione dell'attività.

Nota: se DeviceLock Enterprise Server viene eseguito su Windows NT4, l'utilizzo di Dynamic List richiede l'installazione dell'estensione di Active Directory, che può essere scaricata all'indirizzo: http://www.microsoft.com/downloads/details.aspx?FamilyID=7c219dcc-ec00-4c98-ba61-fd98467952a8.



Nel parametro **Path**, è necessario specificare un percorso verso il contenitore da cui verranno recuperati i computer al momento dell'esecuzione dell'attività. È necessario utilizzare la rappresentazione stringa LDAP per i nomi distinti.

È possibile sfogliare la struttura delle directory e scegliere il contenitore desiderato premendo il pulsante **Select**. In questo caso, un percorso verso il contenitore viene specificato automaticamente nel parametro **Path**.

Selezionare il flag **Traverse subcontainers when enumerating computers** per consentire a DeviceLock Enterprise Server di recuperare i computer da tutti i contenitori nidificati inclusi nel contenitore selezionato. Se il flag non viene selezionato, tutti i contenitori nidificati vengono ignorati e solo i computer ubicati direttamente nel contenitore selezionato vengono recuperati al momento dell'esecuzione dell'attività.

Sono presenti due modalità di utilizzo del servizio di directory:

- **Active Directory** – Sfogliare la struttura di Active Directory e selezionare il contenitore desiderato.

  Sebbene sia possibile visualizzare la struttura di Active Directory anche tramite l'opzione **LDAP** (vedere in basso), la modalità Active Directory consente di ottenere risultati più efficaci tra i servizi di directory e DeviceLock Enterprise Server e, di conseguenza, di utilizzare meno risorse.

  Se occorre immettere credenziali alternative per accedere ad Active Directory, premere il pulsante **...** per aprire la finestra di dialogo

Credentials e specificare l'account utente e la password corrispondente.

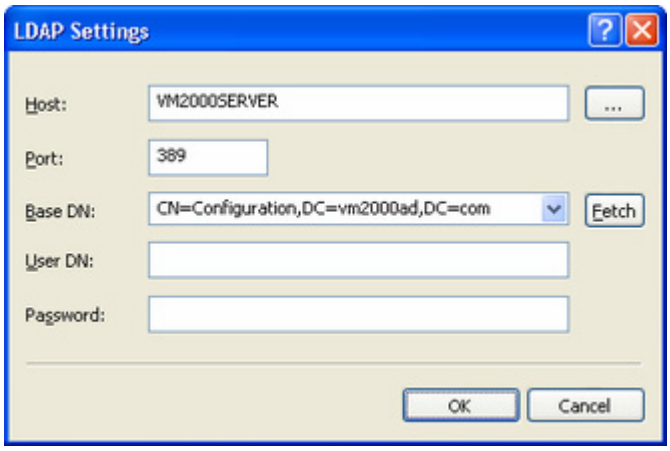
Nota: se si effettua l'accesso ad Active Directory senza specificare credenziali alternative, DeviceLock Enterprise Server utilizza le credenziali dell'account con cui è stato avviato il servizio. Per ulteriori informazioni, leggere la descrizione del parametro Log on as.

Selezionare il flag **Synchonization** per consentire a DeviceLock Enterprise Server di utilizzare i meccanismi di sincronizzazione interni forniti da Active Directory. In tal modo è possibile ridurre drasticamente il carico di lavoro del controller di dominio e di velocizzare il processo di recupero dei computer durante l'esecuzione dell'attività.

Nota: per utilizzare la funzione di sincronizzazione, è necessario l'accesso amministrativo.

- **LDAP** – Sfogliare la struttura di LDAP (Lightweight Directory Access Protocol) e selezionare il contenitore desiderato.

  Per configurare una connessione al server LDAP, premere il pulsante **...** e aprire la finestra di dialogo **LDAP Settings**.



  Host – nome o indirizzo IP del server LDAP verso cui effettuare la connessione.

  Port – porta TCP in cui il server LDAP accetta le connessioni. La porta predefinita è 389.

  Base DN – il punto iniziale per la navigazione nella struttura delle directory. È necessario utilizzare la rappresentazione stringa LDAP per i nomi distinti (ad esempio cn=qa,o=SMARTLINE,c=US). Lasciare vuoto il campo **Base DN** per iniziare a sfogliare dalla struttura.

  Premere il pulsante **Fetch** per ottenere tutti i contesti dei nomi pubblicati.

  User DN – nome distinto utilizzato dall'utente per collegarsi alla directory. È necessario utilizzare la rappresentazione stringa LDAP per i nomi distinti (ad esempio cn=admin,o=SMARTLINE,c=US).

Nota: se si effettua l'accesso al server LDAP senza specificare un utente, DeviceLock Enterprise Server utilizza le credenziali dell'account con cui è stato avviato il servizio. Per ulteriori informazioni, leggere la descrizione del parametro Log on as.

Password – la password dell'utente.

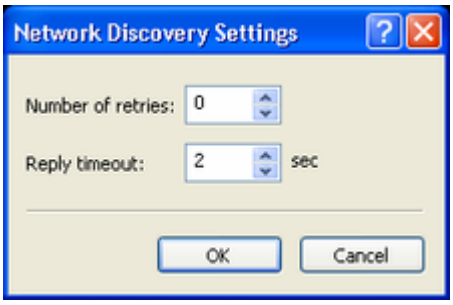
Network discovery methods – tipi di scansione di rete utilizzati per determinare lo stato (**available** o **unavailable**) dei computer monitorati.

Durante l'esecuzione dell'attività, DeviceLock Enterprise Server utilizza tutti i metodi di rilevamento selezionati nell'ordine specificato, fino a quanto non viene restituito lo stato available per il computer di destinazione. Se nessun metodo selezionato restituisce lo stato **available**, il computer di destinazione riceve lo stato **unavailable**.

Sono supportati tre tipi di scansione di rete:

1. **Ping sweep** – DeviceLock Enterprise Server invia un ping ICMP regolare al computer di destinazione e aspetta la sua risposta.
2. **NetBIOS queries** – se sul computer di destinazione è installato il Client per reti Microsoft, tale computer risponde alla query di tipo NetBIOS inviata da DeviceLock Enterprise Server.
3. **TCP discovery (ports)** – DeviceLock Enterprise Server cerca una specifica porta TCP aperta nel computer di destinazione. Utilizzando una virgola (,) o un punto e virgola (;) come separatore è possibile indicare più porte, che verranno verificate una ad una nell'ordine specificato.

Nota: in presenza di un firewall attivo su un computer di destinazione, l'invio di tutti o alcuni dei pacchetti di rete potrebbe essere bloccato; in tal caso, un computer viene considerato non disponibile anche se è acceso e attivo.



Per definire parametri aggiuntivi per i metodi di rilevamento, premere il pulsante **Advanced settings** e aprire la finestra di dialogo **Network Discovery Settings**.

Number of retries – numero di volte per cui DeviceLock Enterprise Server esegue ciascun tipo di scansione quando torna nello stato **unavailable**. 0 significa che non vengono eseguiti ulteriori tentativi per questo tipo di scansione dopo il fallimento del primo tentativo.

Reply timeout – il tempo in secondi durante il quale DeviceLock Enterprise Server attende una risposta da parte del computer di destinazione per ciascun tipo di scansione. Se DeviceLock Enterprise Server è in esecuzione su una rete lenta od occupata, è consigliabile aumentare il tempo impostato.

Service connection settings – queste opzioni definiscono la modalità di connessione di DeviceLock Enterprise Server ai DeviceLock Service sul computer monitorato, al fine di ottenere la versione del servizio, le impostazioni, ecc. Se non vengono specificate le impostazioni di connessione corrette, DeviceLock Enterprise Server non è in grado di collegarsi ai servizi monitorati e i computer di questi ultimi non ricevono lo stato **available**.

DeviceLock Service può essere configurato per utilizzare una porta fissa o porte dinamiche durante la procedura di installazione. Per ulteriori informazioni al riguardo, leggere le sezioni Installazione automatica e Installazione remota tramite DeviceLock Enterprise Manager del presente manuale.

Sono disponibili due opzioni di connessione:

- **Dynamic ports** – se si desidera indicare a DeviceLock Enterprise Server di utilizzare le porte dinamiche per le comunicazioni con DeviceLock Service, selezionare questa opzione.
- **Fixed TCP port** – se DeviceLock Service viene configurato per accettare le connessioni su una porta fissa, selezionare questa opzione e specificare il numero di porta.

Nota: per connettersi correttamente ai DeviceLock Service e ottenere le informazioni necessarie, DeviceLock Enterprise Server deve disporre almeno dei diritti di accesso di sola lettura a questi servizi. Se questa attività deve anche scrivere alcune impostazioni sui DeviceLock Service monitorati, DeviceLock Enterprise Server richiede i diritti di accesso completi a questi servizi.

Per connettersi ai DeviceLock Service monitorati, DeviceLock Enterprise Server utilizza le credenziali dell'account con cui è stato avviato il servizio. Può inoltre utilizzare un'autenticazione DeviceLock Certificate, se viene specificata una chiave privata. Per ulteriori informazioni, leggere la descrizione dei parametri Log on as e Certificate Name.

Verify Service Settings – selezionare questo flag se si desidera verificare l'integrità dei criteri per i DeviceLock Service in esecuzione sui computer monitorati.

- **Service Settings file** – per assegnare la serie di criteri principale all'attività, caricare il file XML con le impostazioni del servizio (il file della serie di criteri principale). Questo file della serie di criteri principale può essere creato utilizzando DeviceLock Management Console, DeviceLock Group Policy Manager e/o DeviceLock Service Settings Editor.

  Durante la procedura di verifica dei criteri, DeviceLock Enterprise Server scarica i criteri da ciascun DeviceLock Service monitorato e li confronta con la serie di criteri principale assegnata all'attività.

  Tutti i parametri non configurati (con lo stato **Not Configured**) all'interno della serie di criteri principale vengono ignorati durante la procedura di verifica dei criteri. Utilizzando questa funzione, è possibile monitorare unicamente l'integrità dei parametri più importanti, consentendo la modifica degli altri parametri senza indicarla nel registro di monitoraggio.

Per caricare il file della serie di criteri principale, premere il pulsante **...** Poiché la firma non viene convalidata in questo passaggio, può essere un file firmato o non firmato. Tuttavia, se si carica il file firmato, il suo nome viene visualizzato nel campo **Service Settings file** tra parentesi tonde.

Se si sta modificando l'attività e la serie di criteri principale è già stata assegnata, è possibile esportarla in un file XML esterno premendo il pulsante **Save**.

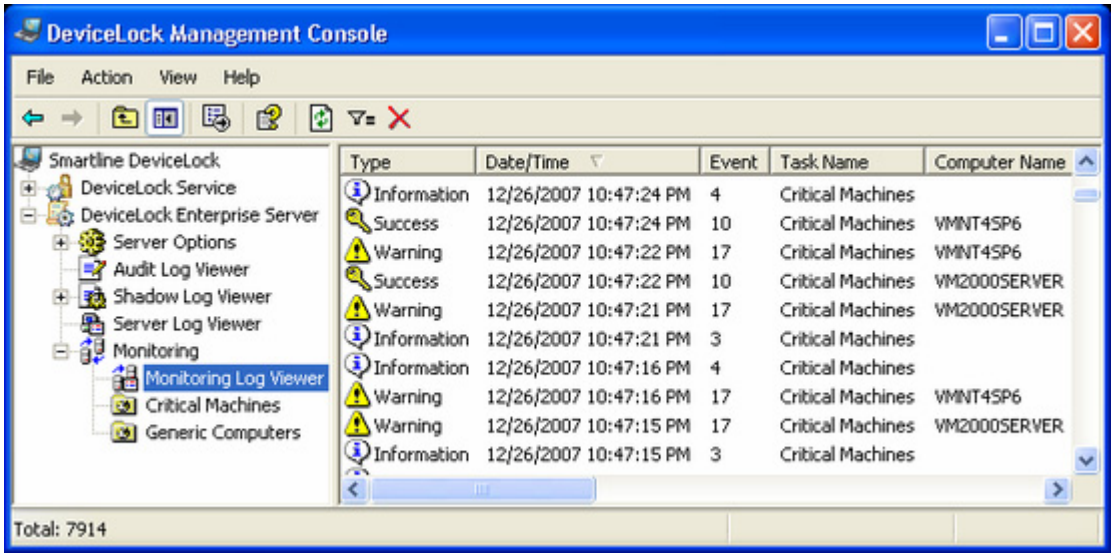
- **Restore Service Settings** – se selezionato, DeviceLock Enterprise Server sovrascrive i criteri correnti di un DeviceLock Service monitorato per cui il processo di verifica delle norme non è andato a buon fine con la serie di norme principale assegnata all'attività. Questa funzionalità, permette di monitorare passivamente l'integrità di parametri specifici e di ripristinarli in caso di modifiche.

Scanning interval – il tempo espresso in secondi che deve trascorrere dalla fine di un'attività all'inizio dell'esecuzione della stessa attività da parte di DeviceLock Enterprise Server.

Number of scanning threads – numero massimo di thread che possono essere utilizzati simultaneamente da questa attività. È possibile aumentare questo numero per parallelizzare il processo di scansione dei computer. Tuttavia, un numero più alto di thread richiede maggiori risorse hardware (in particolare RAM e larghezza di rete) per DeviceLock Enterprise Server.

Monitoring Log Viewer

Questo visualizzatore consente di recuperare il registro di monitoraggio. Quest'ultimo viene utilizzato dalle attività per scrivere dati sui computer e sui DeviceLock Service monitorati.


DeviceLock Management Console
File Action View Help
Smartline DeviceLock
DeviceLock Service
DeviceLock Enterprise Server
Server Options
Audit Log Viewer
Shadow Log Viewer
Server Log Viewer
Monitoring
Monitoring Log Viewer
Critical Machines
Generic Computers
Type Date/Time Event Task Name Computer Name
Information 12/26/2007 10:47:24 PM 4 Critical Machines
Success 12/26/2007 10:47:24 PM 10 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:22 PM 17 Critical Machines VMNT4SP6
Success 12/26/2007 10:47:22 PM 10 Critical Machines VM2000SERVER
Warning 12/26/2007 10:47:21 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:21 PM 3 Critical Machines
Information 12/26/2007 10:47:16 PM 4 Critical Machines
Warning 12/26/2007 10:47:16 PM 17 Critical Machines VMNT4SP6
Warning 12/26/2007 10:47:15 PM 17 Critical Machines VM2000SERVER
Information 12/26/2007 10:47:15 PM 3 Critical Machines
Total: 7914

Descrizione delle colonne del visualizzatore:

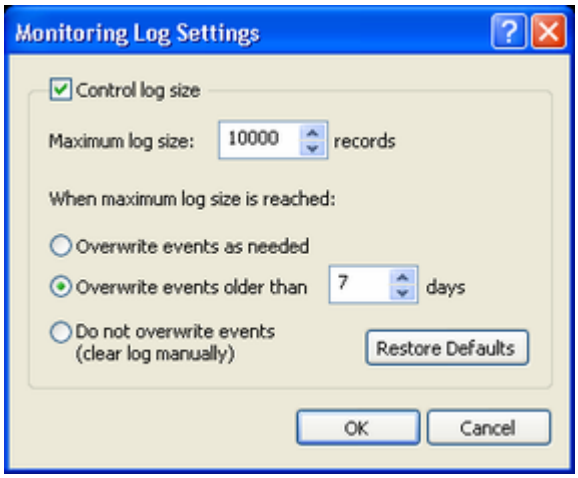
- **Type** – la classe di un evento: **Success**, **Information**, **Warning** o **Error**.
- **Date/Time** – data e ora in cui si è verificato un evento.
- **Event** – numero identificativo di un particolare tipo di evento.
- **Task Name** – nome dell'attività responsabile dell'evento. Se un evento non è collegato a nessuna attività, può essere vuota.
- **Computer Name** – nome del computer che appartiene all'attività responsabile dell'evento. Se un evento non è collegato al computer, può essere vuota.
- **Information** – informazioni specifiche su un evento, ad esempio stato, errore, avviso, ecc.
- **Server** – nome del server in cui si è verificato l'evento.
- **Record N** – numero del record.

Per aggiornare l'elenco, selezionare **Refresh** dal menu contestuale che compare facendo clic con il pulsante destro del mouse o premendo l'apposito pulsante nella barra degli strumenti.

Per cancellare tutti i record dal presente registro, selezionare **Clear** dal menu contestuale o premere l'apposito pulsante nella barra degli strumenti.

Monitoring Log Settings

Per definire una dimensione massima del registro e indicare a DeviceLock Enterprise Server come comportarsi in presenza di un registro pieno, selezionare **Settings** dal menu contestuale di **Monitoring Log Viewer**.

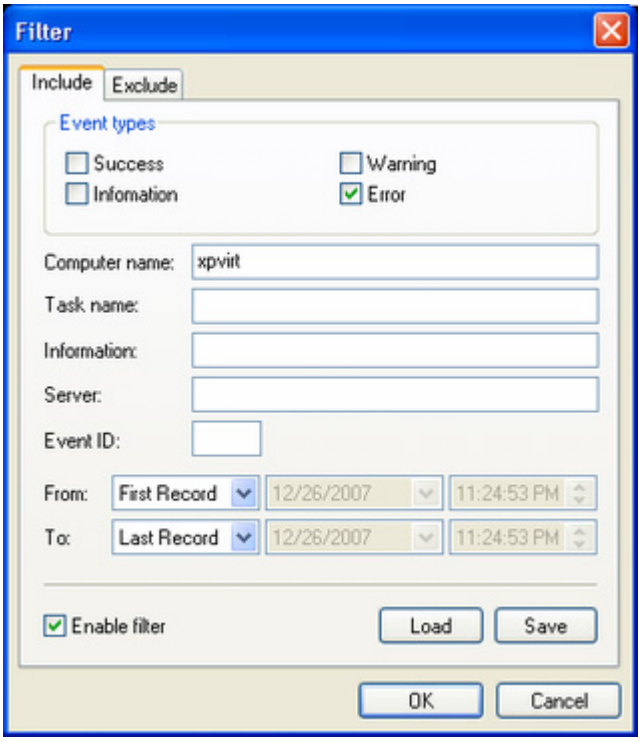


Per informazioni su queste impostazioni, leggere la sezione Audit Log Settings (Server) del presente manuale.

Filtro del registro di monitoraggio

È possibile filtrare i dati di Monitoring Log Viewer in modo tale da visualizzare nell'elenco solo i record che soddisfano determinate condizioni.

Per aprire la finestra di dialogo **Filter**, selezionare **Filter** dal menu contestuale di **Monitoring Log Viewer** o premere l'apposito pulsante nella barra degli strumenti.



Non vi sono differenze sostanziali tra la definizione dei filtro di registro di controllo e di registro di monitoraggio; per ulteriori informazioni, consultare la sezione Audit Log Filter (Service) del presente manuale.

Se il filtro è attivo, è possibile impostarne le condizioni immettendo i valori desiderati nei seguenti campi:

- **Success** – specifica se filtrare o meno gli eventi di classe **Success**.
- **Information** – specifica se filtrare o meno gli eventi di classe **Information**.
- **Warning** – specifica se filtrare o meno gli eventi di classe **Warning**.
- **Error** – specifica se filtrare o meno gli eventi di classe **Error**.

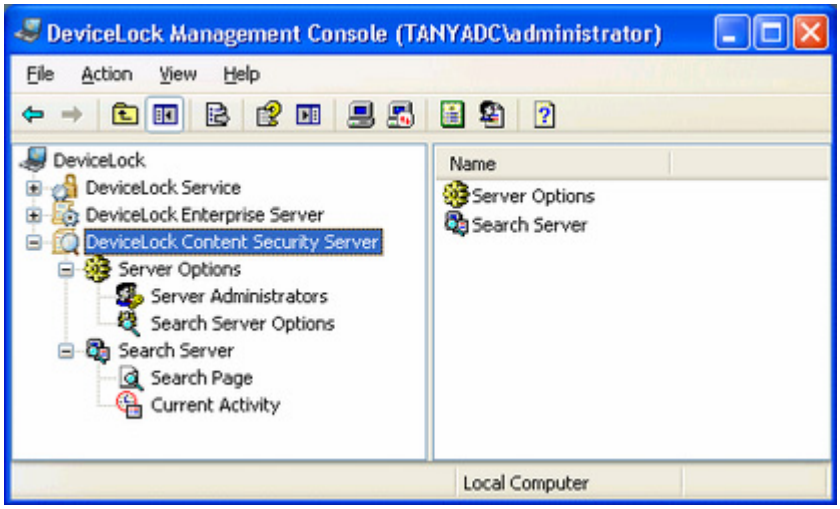
- **Computer Name** – la porzione di testo che corrisponde a un valore nella colonna **Computer Name** di Monitoring Log Viewer. Il campo non distingue tra maiuscole e minuscole ed è possibile utilizzare caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Task Name** – la porzione di testo che corrisponde a un valore nella colonna **Task Name** di Monitoring Log Viewer. Il campo non distingue tra maiuscole e minuscole ed è possibile utilizzare caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Information** – la porzione di testo che corrisponde a un valore nella colonna **Information** di Monitoring Log Viewer. Il campo non distingue tra maiuscole e minuscole ed è possibile utilizzare caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Server** – la porzione di testo che corrisponde a un valore nella colonna **Server** di Monitoring Log Viewer. Il campo non distingue tra maiuscole e minuscole ed è possibile utilizzare caratteri jolly.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **Event ID** – il numero che corrisponde a un valore nella colonna **Event** di Monitoring Log Viewer.
  È possibile inserire più valori separandoli con un punto e virgola (;).
- **From** – specifica l'inizio dell'intervallo di eventi da filtrare. Selezionare **First Event** per visualizzare gli eventi a partire dal primo evento inserito nel registro. Selezionare **Events On** per visualizzare gli eventi a partire da una data e ora specifiche.
- **To** – specifica la fine dell'intervallo di eventi da filtrare. Selezionare **Last Event** per visualizzare gli eventi fino all'ultimo evento inserito nel registro. Selezionare **Events On** per visualizzare gli eventi che si sono verificati fino a una data e ore specifiche.

Gestione e utilizzo di DeviceLock Content Security Server

Esplorazione di DeviceLock Content Security Server

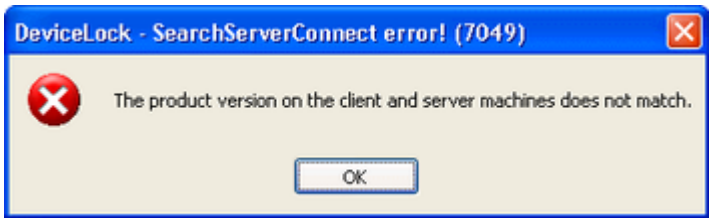
Prima di accedere alle funzionalità di DeviceLock Content Security Server, ecco alcune informazioni sull'esplorazione dell'interfaccia.

Utilizzare il nodo **DeviceLock Content Security Server** in DeviceLock Management Console per configurare e utilizzare DeviceLock Content Security Server.



Fare clic con il pulsante destro del mouse sul nodo **DeviceLock Content Security Server** per visualizzare i seguenti comandi:

- **Connect**: consente di effettuare la connessione al computer su cui viene eseguito DeviceLock Content Security Server. Per ulteriori informazioni, consultare la sezione "Connessione ai computer".
  In caso di connessione a un computer su cui è installata una versione precedente di DeviceLock Content Security Server, potrebbe essere visualizzato il seguente messaggio:

  In tal caso, è necessario installare la versione aggiornata di DeviceLock Content Security Server sul computer. Per informazioni sull'installazione di DeviceLock Content Security Server, consultare la sezione "Installazione di DeviceLock Content Security Server".

- **Reconnect**: consente di effettuare la connessione al computer attualmente collegato.
- **Connect to Last Used Server at Startup**: fare clic su questo comando per indicare a DeviceLock Management Console di collegarsi automaticamente all'ultimo server utilizzato a ogni avvio della console.
- **Certificate Generation Tool**: avvia l'apposito strumento che consente di generare i certificati di DeviceLock. Per ulteriori informazioni, consultare la sezione "Creazione dei certificati di DeviceLock".

- **DeviceLock Signing Tool**: avvia l'apposito strumento che consente di concedere agli utenti un accesso temporaneo ai dispositivi richiesti e di firmare i file XML con le impostazioni di DeviceLock Service. Per ulteriori informazioni, consultare la sezione "Strumento DeviceLock Signing".
- **About DeviceLock**: apre le finestra di dialogo contenente le informazioni sulla versione DeviceLock e sulle licenze possedute.

Espandere il nodo **DeviceLock Content Security Serve**r per visualizzare i seguenti sottonodi:

- Nodo **Server Options**. Utilizzare questo nodo per configurare DeviceLock Content Security Server e Search Server.

  Il seguente elenco descrive le impostazioni generali di DeviceLock Content Security Sever che possono essere configurate:

  - **Server Administrators**: utilizzare questa impostazione per specificare i membri del gruppo di amministratori di server e i relativi diritti di accesso.
  - **DeviceLock certificate**: utilizzare questa impostazione per installare o rimuovere il certificato di DeviceLock.
  - **Service startup account**: utilizzare questa impostazione per specificare le informazioni dell'account di avvio (ad esempio nome e password) per il servizio del server.
  - **TCP port**: utilizzare questa impostazione per specificare la porta TCP utilizzata dal server per collegarsi a DeviceLock Management Console.

  Il seguente elenco descrive le impostazioni relative alla ricerca full-text che è possibile configurare per Search Server:

  - **DeviceLock Enterprise Server(s)**: utilizzare questa impostazione per specificare i DeviceLock Enterprise Server i cui dati verranno indicizzati per la ricerca full-text.
  - **Index directory**: utilizzare questa impostazione per specificare la posizione dell'indice full-text.
  - **Indexing interval**: utilizzare questa impostazione per specificare l'intervallo temporale, espresso in minuti, che va dalla fine di un processo di indicizzazione all'avvio del processo successivo.
  - **Merge Interval**: utilizzare questa impostazione per specificare l'intervallo di tempo (in minuti) per l'esecuzione delle operazioni di unione.
  - **Extract text from binary**: utilizzare questa impostazione per autorizzare o impedire all'indice di includere le informazioni testuali dai dati binari.
  - **Search Server License(s)**: utilizzare questa impostazione per installare il numero richiesto di licenze di Search Server.

- Nodo **Search Server**. Utilizzare questo nodo per avviare un'operazione di ricerca e per monitorare l'attività di indicizzazione corrente.

Configurazione delle impostazioni generali di DeviceLock Content Security Server

Sono disponibili due tipi di impostazioni per DeviceLock Content Security Server:

- **Impostazioni generali di DeviceLock Content Security Server.** Queste impostazioni influenzano l'utilizzo complessivo di DeviceLock Content Security Server.
- **Impostazioni di Search Server relative alla ricerca full-text.** Queste impostazioni riguardano la funzionalità di ricerca full-text e influiscono solo sul componente Search Server di DeviceLock Content Security Server. Per ulteriori informazioni, consultare la sezione "Configurazione della ricerca full-text di Search Server".

È possibile configurare le impostazioni generali del server durante l'installazione iniziale di DeviceLock Content Security Server oppure utilizzare DeviceLock Management Console per configurare e/o modificare le impostazioni dopo l'installazione e l'esecuzione del server.

Nota: per utilizzare e gestire DeviceLock Content Security Server, occorre essere membri del gruppo di amministratori di server e disporre dei diritti sufficienti.

Per utilizzare DeviceLock Management Console, è necessario collegare quest'ultima al computer su cui DeviceLock Content Security Server è installato e in esecuzione. Per farlo, nella struttura della console fare clic con il pulsante destro del mouse su **DeviceLock Content Security Server** e selezionare **Connect**. Per ulteriori informazioni, consultare la sezione "Connessione ai computer".

In DeviceLock Management Console è possibile eseguire le seguenti configurazioni:

- Specificare gli utenti che possono accedere a DeviceLock Content Security Server.
- Modificare le informazioni dell'account di avvio (ad esempio nome e password) per il servizio DeviceLock Content Security Server.
- Installare o rimuovere il certificato di DeviceLock utilizzato per autenticare le comunicazioni tra DeviceLock Content Security Server e DeviceLock Enterprise Server.
- Modificare la porta TCP utilizzata da DeviceLock Content Security Server per collegarsi a DeviceLock Management Console.

È possibile eseguire tali attività singolarmente o in gruppo.

Per eseguire le attività in gruppo, è possibile utilizzare la configurazione guidata di DeviceLock Content Security Server, che viene avviata automaticamente durante l'installazione o l'aggiornamento di DeviceLock Content Security Server.

Per eseguire le attività di configurazione in gruppo

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, fare clic con il pulsante destro del mouse su **Server Options** e selezionare **Properties**.

   Viene visualizzata la prima pagina della configurazione guidata.

3. Seguire le istruzioni visualizzate. Una volta completata ciascuna pagina, passare alla pagina successiva facendo clic su **Next** o tornare indietro selezionando **Back**. Fare clic su **Finish** nell'ultima pagina per completare la configurazione guidata.

   Per informazioni dettagliate su come configurare DeviceLock Content Security Server utilizzando la configurazione guidata, consultare la sezione "Installazione di DeviceLock Content Security Server".

Seguono le istruzioni dettagliate su come eseguire le singole attività di configurazione utilizzando DeviceLock Management Console.

Attività: configurare gli utenti che possono accedere a DeviceLock Content Security Server

È possibile selezionare gli utenti che possono accedere al proprio DeviceLock Content Security Server. In tal modo si evita che estranei possano accedere al server o danneggiare il contenuto dello stesso.

Per specificare gli utenti che possono accedere al server

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, eseguire una delle seguenti azioni:

   - Selezionare **Server Options**. Nel riquadro dei dettagli, fare doppio clic su **Server Administrators** oppure fare clic con il pulsante destro del mouse su **Server Administrators** e selezionare **Properties**.
     Dopo aver selezionato Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

     - OPPURE -
   - Espandere **Server Options**. In **Server Options**, fare clic con il pulsante destro del mouse su **Server Administrators** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Content Security Server.

3. Nella finestra di dialogo **DeviceLock Content Security Server**, eseguire una delle seguenti azioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Per attivare la protezione predefinita	• Selezionare la casella di controllo **Enable Default Security**. *Se viene attivata questa opzione, gli utenti che appartengono al gruppo locale degli amministratori dispongono dell'accesso completo a DeviceLock Content Security Server*.
Per limitare l'accesso al server agli utenti specificati	1. Deselezionare la casella di controllo **Enable Default Security**. 2. In **Users**, fare clic su **Add** per aggiungere gli utenti autorizzati ad accedere a DeviceLock Content Security Server. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 3. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi selezionati vengono aggiunti al gruppo di amministratori di server e vengono visualizzati sotto Users nella finestra di dialogo DeviceLock Content Security Server. Gli amministratori di server sono utenti o gruppi autorizzati a configurare e utilizzare DeviceLock Content Security Server. Per impostazione predefinita, i membri del gruppo di amministratori di server dispongono dei diritti di accesso completi al server.* Per modificare i loro diritti di accesso, in **Users**, selezionare l'utente o il gruppo desiderato e fare clic sull'opzione desiderata nell'elenco dei diritti di accesso. Le opzioni disponibili sono: **Full Access**: attiva l'accesso completo a DeviceLock Content Security Server. Gli utenti possono installare/disinstallare DeviceLock Content Security Server, collegarsi a quest'ultimo utilizzando DeviceLock Management Console, modificarne le impostazioni e inoltrare query di ricerca. **Change**: attiva l'accesso a DeviceLock Content Security Server con possibilità di modifica. Gli utenti possono installare/disinstallare DeviceLock Content Security Server, collegarsi a quest'ultimo utilizzando DeviceLock Management Console, modificarne le impostazioni e inoltrare query di ricerca. Tuttavia, non possono aggiungere/rimuovere utenti nel/dal gruppo di amministratori di server né modificare i diritti di accesso concessi agli amministratori di server. **Read-only**: attiva l'accesso di sola lettura a DeviceLock Content Security Server. Gli utenti possono collegarsi a DeviceLock Content Security Server utilizzando DeviceLock Management Console, inoltrare query di ricerca e visualizzare le impostazioni, me non possono modificare le impostazioni né creare un nuovo indice per Search Server.

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
	Nota: è preferibile che i membri del gruppo di amministratori di server dispongano di privilegi di amministratore locale. Per rimuovere un utente o un gruppo dal gruppo di amministratori di server, in **Users** selezionare l'utente o il gruppo e fare clic su **Delete**. *È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi*.

4. Fare clic su **OK**.

Attività: modificare l'account di avvio del servizio o della password

Con il passare del tempo, potrebbe essere necessario modificare l'account specificato per l'avvio del servizio di DeviceLock Content Security Server durante il processo di installazione. È inoltre possibile modificare la password dell'account di avvio del servizio.

Per modificare l'account di avvio del servizio o la password

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, selezionare **Server Options**.

   Dopo aver selezionato Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **Service startup account** oppure fare clic con il pulsante destro del mouse su **Service startup account** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Content Security Server.

4. Nella finestra di dialogo **DeviceLock Content Security Server**, eseguire una delle seguenti azioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Per modificare l'account di avvio del servizio	1. Nella sezione **Log on as**, fare clic su **Browse**. *Viene visualizzata la finestra di dialogo Select User*. 2. Nella finestra di dialogo **Select User**, nella casella **Enter the object name to select**, digitare il nome dell'utente, quindi fare clic su **OK**. *L'utente selezionato viene visualizzato nella casella This account della finestra di dialogo DeviceLock Content Security Server*.

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
	Si consiglia di utilizzare un account dotato di privilegi amministrativi su tutti i computer in cui viene eseguito DeviceLock Enterprise Server. In un ambiente di dominio, si consiglia di utilizzare un account utente appartenente al gruppo di amministratori di dominio. In caso contrario, è necessario ricorrere all'autenticazione tramite il certificato di DeviceLock.
Per modificare la password dell'account del servizio	1. Nella sezione **Log on as**, digitare la nuova password nella casella **Password**. 2. Digitare nuovamente la password nella casella **Confirm password**.
Per assegnare l'account di sistema locale al servizio del server	• Nella sezione **Log on as**, fare clic sull'account **Local System account**. *Se il servizio utilizza questo account, non può accedere a DeviceLock Enterprise Server in esecuzione su un computer remoto e deve ricorrere al certificato DeviceLock Certificate per eseguire l'autenticazione sul computer*.

5. Fare clic su **OK**.

Attività: installare o rimuovere il certificato di DeviceLock utilizzato per autenticare le comunicazioni tra DeviceLock Content Security Server e DeviceLock Enterprise Server

In alcune situazioni, l'account utente con cui viene eseguito DeviceLock Content Security Server non può effettuare l'accesso remoto a DeviceLock Enterprise Server. In casi del genere, è possibile ricorrere all'autenticazione tramite il certificato di DeviceLock. Per farlo, installare la stessa chiave privata del certificato di DeviceLock su DeviceLock Content Security Server e DeviceLock Enterprise Server. Per informazioni dettagliate sui certificati di DeviceLock, consultare la sezione "Certificati di DeviceLock".

Per installare o rimuovere DeviceLock Certificate su DeviceLock Content Security Server

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, selezionare **Server Options**.

   Dopo aver selezionato Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **DeviceLock certificate** oppure fare clic con il pulsante destro del mouse su **DeviceLock certificate** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Content Security Server.

4. Nella finestra di dialogo **DeviceLock Content Security Server**, eseguire una delle seguenti azioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Per installare la chiave privata del certificato di DeviceLock	1. Accanto alla casella **Certificate Name**, fare clic sul pulsante dei punti di sospensione ... per aprire la finestra di dialogo **Select the DeviceLock Certificate file** e cercare il file da usare. 2. Nella finestra di dialogo **Select the DeviceLock Certificate file**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file del certificato. 3. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file del certificato. 4. Fare clic sul file, quindi scegliere **Open**. *Il nome del certificato viene visualizzato nella casella Certificate Name della finestra di dialogo DeviceLock Content Security Server*.
Per rimuovere la chiave privata del certificato di DeviceLock	• Fare clic su **Remove** accanto alla casella **Certificate Name**.

5. Fare clic su **OK**.

Attività: modificare la porta TCP utilizzata per effettuare il collegamento a DeviceLock Management Console

Con il passare del tempo, potrebbe essere necessario modificare la porta TCP utilizzata da DeviceLock Content Security Server per collegarsi a DeviceLock Management Console.

Per modificare la porta TCP utilizzata per effettuare il collegamento a DeviceLock Management Console

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, selezionare **Server Options**.

   Dopo aver selezionato Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **TCP port** oppure fare clic con il pulsante destro del mouse su **TCP port** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Content Security Server.

4. Nella sezione **Connection Settings** della finestra di dialogo **DeviceLock Content Security Server**, eseguire una delle seguenti azioni:

   - Fare clic su **Dynamic ports** per configurare DeviceLock Content Security Server in modo tale da utilizzare una porta dinamica.

- OPPURE -

- Fare clic su **Fixed TCP port** per configurare DeviceLock Content Security Server in modo tale da utilizzare una porta statica. In seguito, digitare il numero della porta nella casella **Fixed TCP port**.
  Per impostazione predefinita, DeviceLock Content Security Server comunica attraverso la porta TCP 9134.

5. Fare clic su **OK**.

Configurazione della ricerca full-text per Search Server

Queste impostazioni riguardano la funzionalità di ricerca full-text e si applicano solo al componente Search Server di DeviceLock Content Security Server.

Durante l'installazione di DeviceLock Content Security Server, è possibile installare unicamente le licenze di Search Server. Utilizzare DeviceLock Management Console per definire tutte le opzioni di configurazione di Search Server.

In DeviceLock Management Console è possibile eseguire le seguenti configurazioni:

- Installare il numero richiesto di licenze di Search Server.
- Specificare i DeviceLock Enterprise Server i cui dati verranno indicizzati per la ricerca full-text.
- Specificare la posizione dell'indice full-text.
- Autorizzare o impedire all'indice di includere le informazioni testuali dai dati binari.
- Pianificare l'indicizzazione full-text.
- Configurazione della pianificazione delle operazioni di unione.
- Ricreare immediatamente l'indice full-text.
- Aggiornare immediatamente l'indice esistente.
- Monitorare e aggiornare lo stato dell'attività di indicizzazione corrente.

Attività: installare il numero richiesto di licenze di Search Server

È necessario acquistare una licenza speciale di Search Server per DeviceLock Content Security Server. È possibile utilizzare la stessa licenza su un numero illimitato di computer in cui viene eseguito DeviceLock Content Security Server.

Il modello di licenza di Search Server si basa sul numero di voci di registro da indicizzare per la ricerca full-text. Ogni licenza consente a Search Server di indicizzare 1.000 voci dai registri shadowing (Shadow Log e Deleted Shadow Log) e 5000 voci da ogni altro registro (Audit Log, Server Log e Monitoring Log).

A seconda del numero di voci di registro sui DeviceLock Enterprise Server in uso, è possibile acquistare le licenze necessarie. Se si utilizzano più licenze per Search Server, è possibile indicizzare il numero di voci di registro consentito dalle licenze

combinate. Il periodo di prova di DeviceLock Content Security Server è di 30 giorni. Durante il periodo di prova, Search Server può indicizzare 2.000 voci dai registri shadowing e 10.000 voci da ogni altro registro. È possibile acquistare e installare licenze di Search Server aggiuntive in qualsiasi momento.

Per installare le licenze di Search Server

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **Search Server License(s)** oppure fare clic con il pulsante destro del mouse su **Search Server License(s)** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Content Security Server.

4. Nella finestra di dialogo **DeviceLock Content Security Server**, fare clic su **Load License(s)** per cercare il file della licenza.
5. Nella finestra di dialogo **Select the DeviceLock license file**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file della licenza.
6. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file della licenza.
7. Fare clic sul file, quindi scegliere **Open**.

   Le informazioni sui file di licenza sono visualizzate nell'area License information della finestra di dialogo DeviceLock Content Security Server.

   È possibile installare tutte le licenze necessarie per rispondere alle esigenze della propria organizzazione. Per farlo, aggiungere una licenza alla volta.

8. Fare clic su **OK**.

Attività: specificare i DeviceLock Enterprise Server i cui dati verranno indicizzati per la ricerca full-text

Per avviare il processo di creazione dell'indice full-text, è necessario specificare i DeviceLock Enterprise Server i cui dati verranno indicizzati. Search Server avvia automaticamente il processo di indicizzazione non appena vengono specificati i DeviceLock Enterprise Server.

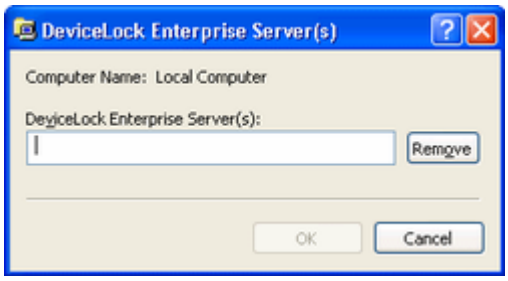
Per specificare i DeviceLock Enterprise Server

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **DeviceLock Enterprise Server(s)** oppure fare clic con il pulsante destro del mouse su **DeviceLock Enterprise Server(s)** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo DeviceLock Enterprise Server(s).



4. Nella finestra **DeviceLock Enterprise Server(s)**, digitare l'indirizzo IR o il nome del computer su cui viene eseguito DeviceLock Enterprise Server.

   I nomi di computer o gli indirizzi IP multipli vanno separati da un punto e virgola (;).

   Nota: verificare che DeviceLock Enterprise Server sia correttamente installato e accessibile da DeviceLock Content Security Server, altrimenti i suoi dati non verranno indicizzati da Search Server.

   Per rimuovere nomi di computer o indirizzi IP, fare clic su **Remove**.

5. Fare clic su **OK**.

Attività: specificare la posizione dell'indice full-text.

È possibile specificare la posizione dell'indice full-text. Se non viene specificata una posizione, l'indice full-text viene creato nella directory predefinita ***%ProgramFiles%\DeviceLock Content Security Server\Index***. Search Server avvia automaticamente il processo di indicizzazione ogni volta che viene specificata una diversa posizione.

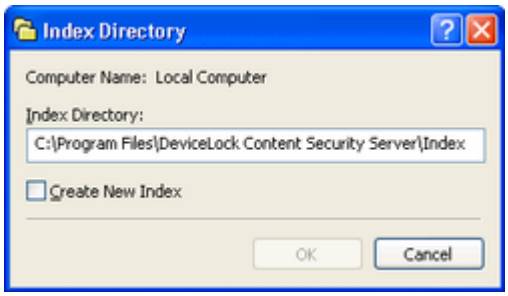
Per specificare la posizione dell'indice

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **Index directory** oppure fare clic con il pulsante destro del mouse su **Index Directory** e selezionare **Properties**.

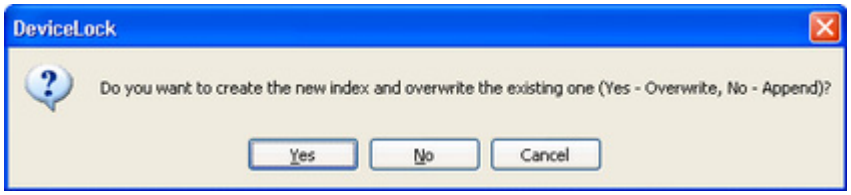
   Viene visualizzata la finestra di dialogo Index Directory.



4. Nella casella **Index Directory** della finestra di dialogo **Index Directory**, digitare il percorso da utilizzare come posizione predefinita dell'indice.

   Se si desidera creare immediatamente un nuovo indice, selezionare la casella di controllo **Create New Index**.

   Se l'indice è già esistente nella posizione specificata e si sceglie di crearne uno nuovo, viene visualizzato il seguente messaggio:



   Nella finestra di messaggio, fare clic su **Yes** per ricreare l'indice full-text. Fare clic su **No** per aggiornare l'indice full-text esistente con le modifiche apportate.

5. Fare clic su **OK**.

Attività: autorizzare o impedire all'indice di includere le informazioni testuali dai dati binari

È possibile autorizzare o impedire all'indice di includere le informazioni testuali dai dati binari.

Per attivare o disattivare l'estrazione di testo dai dati binari

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **Extract text from binary** oppure fare clic con il pulsante destro del mouse su **Extract text from binary** e selezionare **Enable** o **Disable**.

Attività: pianificare l'indicizzazione full-text

L'indicizzazione full-text consente di creare e aggiornare l'indice full-text.

È possibile pianificare il processo di indicizzazione affinché venga avviato automaticamente a intervalli predefiniti. La pianificazione dell'indicizzazione full-text si basa sull'intervallo di indicizzazione. L'intervallo di indicizzazione specifica l'intervallo temporale, espresso in minuti, che va dalla fine di un processo di indicizzazione all'avvio del processo successivo. L'intervallo di indicizzazione predefinito è di 60 minuti.

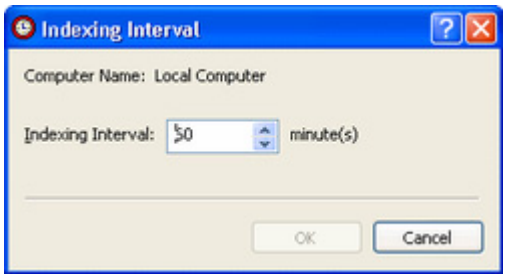
Per pianificare l'indicizzazione full-text

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, fare doppio clic su **Indexing interval** oppure fare clic con il pulsante destro del mouse su Indexing interval e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo Indexing interval.



4. Nella casella **Indexing Interval** della finestra di dialogo **Indexing Interval**, digitare o selezionare il numero di minuti dell'intervallo di indicizzazione.
5. Fare clic su **OK**.

Attività: Configurazione della pianificazione delle operazioni di unione

Le operazioni di unione vengono utilizzate per combinare gli indici temporanei in un indice principale permanente, da utilizzare per le query di ricerca. È possibile pianificare il processo di unione affinché venga avviato a intervalli predefiniti. La pianificazione viene configurata in base all'intervallo di unione. Questo intervallo determina la frequenza (in minuti) con cui Search Server combina gli indici temporanei in un indice principale permanente o, in altre parole, con cui viene aggiornato l'indice principale con i nuovi dati durante un'operazione di indicizzazione. Per impostazione predefinita l'unione viene eseguita ogni 10 minuti. L'intervallo di valori che è possibile specificare va da 1 a 1,000,000.

Durante la specifica dell'intervallo di unione, considerare quanto segue:

- Un breve intervallo di unione rende più rapidi gli aggiornamenti dell'indice principale.

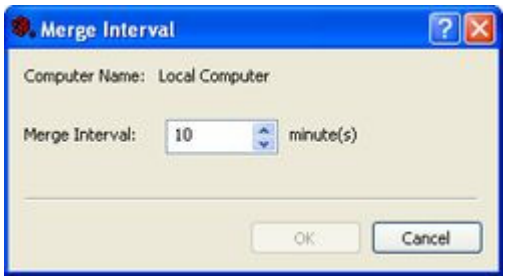
- Non è possibile eseguire ricerche full-text durante il processo di unione.

Per pianificare le operazioni di unione

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Options**.
2. In **Server Options**, selezionare **Search Server Options**.

   Dopo aver selezionato Search Server Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.
3. Nel riquadro dei dettagli, fare doppio clic su **Merge Interval** o fare clic con il pulsante destro del mouse su **Merge Interval** e selezionare **Properties**.

   Viene visualizzata la finestra di dialogo Merge Interval.



4. Nella casella **Merge Interval** della finestra di dialogo **Merge Interval**, digitare o selezionare il numero di minuti dell'intervallo di unione.
5. Fare clic su **OK**.

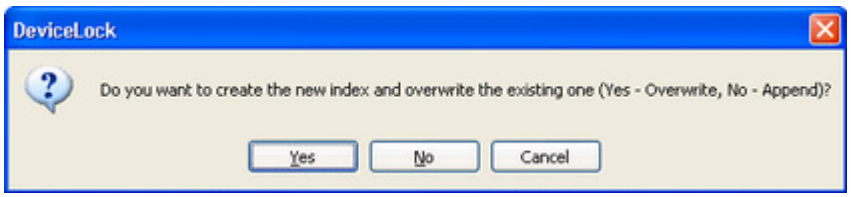
Attività: ricreare immediatamente l'indice full-text

È possibile ricreare l'indice full-text da zero.

Per ricreare immediatamente l'indice full-text

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, fare clic con il pulsante destro del mouse su **Search Server** e selezionare **Create New Index**.

   Se l'indice è già esistente e si sceglie di crearne uno nuovo, viene visualizzato il seguente messaggio:



   Nella finestra di messaggio, fare clic su **Yes** per ricreare l'indice full-text. Fare clic su **No** per aggiornare l'indice full-text esistente con le modifiche apportate.

Attività: aggiornare immediatamente l'indice esistente

Se vengono aggiunti nuovi dati a DeviceLock Enterprise Server e si desidera aggiornare immediatamente l'indice full-text esistente con le modifiche apportate, attenersi alle seguenti istruzioni:

Per aggiornare immediatamente l'indice esistente

1. Nella struttura della console, espandere **DeviceLock Content Security Server**.
2. In **DeviceLock Content Security Server**, fare clic con il pulsante destro del mouse su **Search Server** e selezionare **Index Now**.

   Durante l'aggiornamento, Search Server non ricrea completamente l'indice, ma indicizza unicamente i nuovi dati su DeviceLock Enterprise Server per aggiungere le nuove voci all'indice esistente.

Attività: monitorare e aggiornare lo stato dell'attività di indicizzazione corrente

Le operazioni di indicizzazione full-text possono richiedere molto tempo e l'utilizzo di numerose risorse. Search Server consente di monitorare l'avanzamento delle operazioni di indicizzazione in corso.

Il processo di indicizzazione è composto da due fasi. Nella prima fase, Search Server estrae le parole significative dalle copie shadow e dai record di registro e le salva negli indici temporanei per ciascun DeviceLock Enterprise Server specificato. Per ogni indice temporaneo Search Server elabora 1.000 record da ciascun registro.

Nella seconda fase, se il numero di indici temporanei raggiunge 50 o se passano 10 minuti, tutti gli indici temporanei vengono uniti in un indice master permanente che, a sua volta, viene utilizzato per le query di ricerca. Il processo di fusione degli indici temporanei in un indice master viene comunemente chiamato ***merging*** (unione).

Search Server include gli indicatori dell'avanzamento e dello stato delle attività di indicizzazione e unione.

Indicatori dell'avanzamento e dello stato dell'indicizzazione

È possibile verificare il progresso dell'indicizzazione su ciascun DeviceLock Enterprise Server visualizzando l'indicatore di stato e di avanzamento. L'indicatore di stato mostra lo stato dell'operazione di indicizzazione. La seguente tabella mostra i valori possibili di stato e le relative descrizioni.

STATO	DESCRIZIONE
Idle	Indicizzazione non avviata
Waiting	In attesa dell'avvio dell'indicizzazione
Indexing <*log_name*>	Indicizzazione in corso

L'indicatore di avanzamento mostra la percentuale di completamento del processo di indicizzazione.

Indicatori dell'avanzamento dell'unione e dello stato
È possibile verificare il progresso dell'unione visualizzando l'indicatore di stato e di avanzamento. L'indicatore di stato mostra lo stato dell'operazione di unione. La seguente tabella mostra i valori possibili di stato e le relative descrizioni.

STATO	DESCRIZIONE
Idle	Unione non avviata
Merging	Unione in corso
Defragmenting	Compressione (ottimizzazione) dell'indice in corso. Questa operazione consente di ottimizzare la struttura dell'indice, rimovendo i dati obsoleti e deframmentando le strutture di ricerca per migliorare le prestazioni.

L'indicatore di avanzamento mostra la percentuale di completamento del processo di unione.

Per monitorare e aggiornare lo stato dell'attività di indicizzazione corrente

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Server**.
2. In **Search Server**, selezionare **Current Activity**.

   Dopo aver selezionato Current Activity nella struttura della console, gli indicatori dell'avanzamento dell'unione e dello stato vengono visualizzati nel riquadro dei dettagli.

   Poiché lo stato delle operazioni di indicizzazione e unione non viene aggiornato automaticamente, è necessario eseguire un'operazione di aggiornamento.

   Per avviare un'operazione di aggiornamento, eseguire una qualsiasi delle seguenti azioni:

   - Nella struttura della console, fare clic con il pulsante destro del mouse su **Current Activity** e selezionare **Refresh**.
     - OPPURE -
   - Nella struttura della console, selezionare **Current Activity** e fare clic su **Refresh** sulla barra degli strumenti.
     - OPPURE -
   - Nella struttura della console, selezionare **Current Activity**. Nella colonna **Name** del riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi nome di DeviceLock Enterprise Server o **Merge Index** e selezionare **Refresh**.
     - OPPURE -
   - Nella struttura della console, selezionare **Current Activity**. Nel riquadro dei dettagli, selezionare un nome qualsiasi di DeviceLock Enterprise Server o **Merge Index** e fare clic su **Refresh** nella barra

delle applicazioni.

Utilizzo di Search Server

L'utilizzo di Search Server include le seguenti attività:

- Esecuzione di un'operazione di ricerca full-text
- Utilizzo dei risultati di ricerca

Esecuzione di un'operazione di ricerca full-text

Search Server consente di individuare tutte le occorrenze di una parola o di una frase nel database di DeviceLock Enterprise Server. Poiché, in genere, i risultati delle ricerche sono numerosi, è possibile impostare le opzioni disponibili per ottimizzare le ricerca. Le opzioni di ricerca consentono di specificare il modo di visualizzazione dei risultati. Grazie alle opzioni di ricerca è possibile specificare

- Il numero di risultati della ricerca per pagina.
- Come filtrare i risultati della ricerca recuperati. I risultati della ricerca possono essere filtrati per data e per registro. Ad esempio, è possibile limitare il numero di risultati selezionando solo quelli compresi entro un certo intervallo di date o recuperati da determinati registri.

Seguono alcune considerazioni sull'utilizzo della ricerca full-text.

- Per le ricerche non viene rilevata la distinzione tra maiuscole e minuscole.
- È possibile eseguire ricerche di parole e frasi e utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?) nelle query di ricerca. Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità. Per cercare una frase specifica, inserirla all'interno di virgolette doppie. Per cercare più parole, separarle con uno spazio.
  La seguente tabella mostra il tipo di ricerca, alcuni esempi e i relativi risultati.

TIPO DI RICERCA	ESEMPIO	RISULTATI
Parola singola	price	Risultati che inclusono la parola ***price.*** Verranno visualizzati anche le varianti grammaticali, ad esempio ***prices***, ***priced***, ecc.
Frase	confidential information	Risultati che contengono entrambe le singole parole ***confidential*** e ***information*** e non la frase esatta.
	"confidential information"	Risultati che includono la frase esatta ***confidential information***.

TIPO DI RICERCA	ESEMPIO	RISULTATI
Espressione jolly	te?t	Risultati che includono ***test***, ***text***, ecc.
Espressione jolly	mone*	Risultati che includono ***money***, ***monetary***, ecc.
Espressione jolly	*air	Risultati che includono le parole ***fair***, ***impair***, ***affair***, ecc.
Espressione jolly	* assets	Risultati che includono ***monetary assets***, ***liquid assets***, ***fixed assets***, ***current assets***, ecc.

Per eseguire un'operazione di ricerca

1. Nella struttura della console, espandere **DeviceLock Content Security Server**, quindi **Server Server**.
2. In **Search Server**, selezionare **Search Page**.

   La pagina di ricerca viene visualizzata nel riquadro dei dettagli.

3. Nella casella **Search** della pagina di ricerca, digitare la parola o frase da cercare. Per impostare le opzioni di ricerca, fare clic su **Options** e attenersi alle seguenti istruzioni:
   - Per specificare il numero di risultati per pagina, nell'elenco **Display...results per page**, fare clic su una delle seguenti opzioni: **10**, **20**, **30**, **50**, **100**. Il valore predefinito è 20.
   - Per limitare la ricerca a registri di dati specifici, selezionare le caselle di controllo pertinenti nella sezione **Limit results to the following logs**.
     Per impostazione predefinita, Search Server esegue le ricerche nei registri Audit Log, Shadow Log e Deleted Shadow Log.
   - Per filtrare i risultati della ricerca per data, specificare un intervallo di date per limitare le informazioni provenienti dalle fonti di dati. Per farlo, impostare i seguenti parametri:

PARAMETRO	DESCRIZIONE
From	Specifica la parte iniziale dell'intervallo di date in cui eseguire la ricerca. Valori disponibili: **First Record** e **Records On**. Il valore predefinito è **First Record**. Selezionando **First Record**, Search Server recupera i dati iniziando dal primo record scritto sul registro. Selezionando **Records On**, Search Server recupera i dati scritti da una data specifica iniziale in poi.
To	Specifica la parte finale dell'intervallo di date in cui eseguire la ricerca. Valori disponibili: **Last Record** e **Records On**. Il valore predefinito è Last Record. Selezionando **Last Record**, Search Server recupera i dati

PARAMETRO	DESCRIZIONE
	che finiscono con l'ultimo record scritto sul registro. Selezionando **Records On**, Search Server recupera i dati scritti fino a una data finale specifica.

Se viene selezionata l'opzione **Records On**, fare clic sulle caselle **From** e **To** per visualizzare il calendario. Nel calendario, fare clic sul giorno desiderato per selezionarlo. Fare clic sulle frecce singole (**<>**) per sfogliare i mesi e sulle frecce doppie (**<<>>**) per sfogliare gli anni.

4. Fare clic su **Search**.

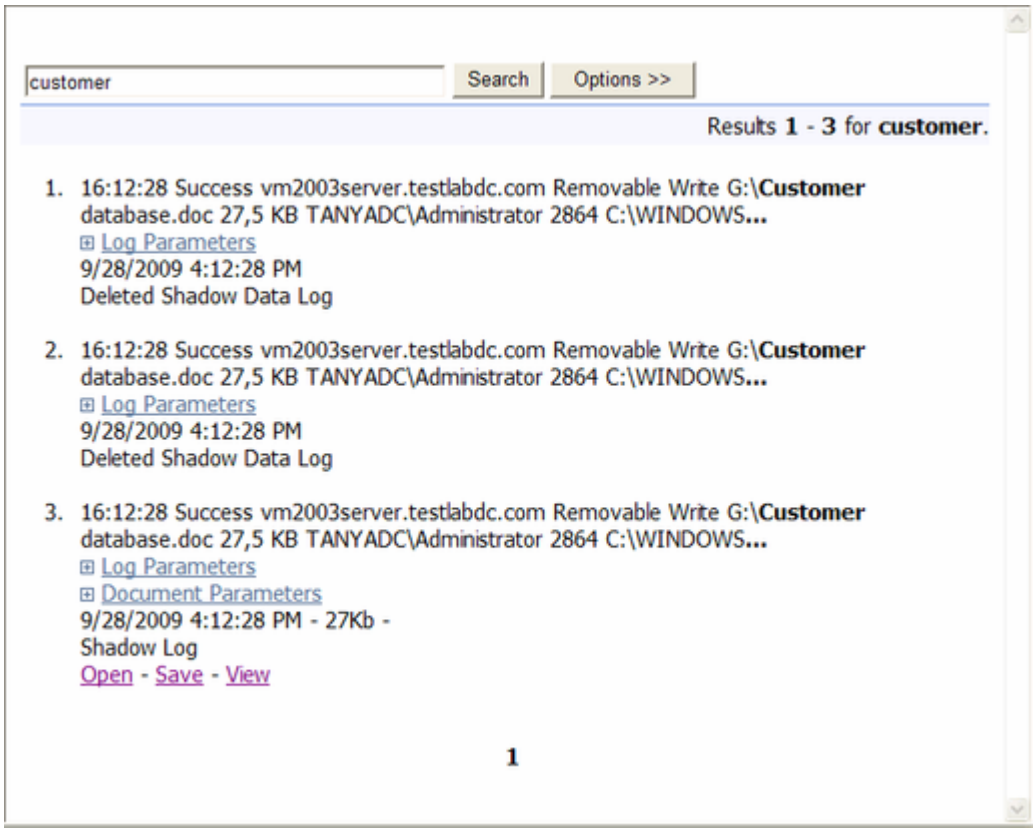
Utilizzo dei risultati di ricerca

L'utilizzo dei risultati di ricerca include le seguenti attività:

- Interpretazione dei risultati di ricerca
- Gestione dei risultati di ricerca recuperati da Shadow Log

Interpretazione dei risultati di ricerca

Dopo aver specificato i criteri e avviato la ricerca, Search Server mostra i risultati della ricerca in una pagina simile alla seguente.

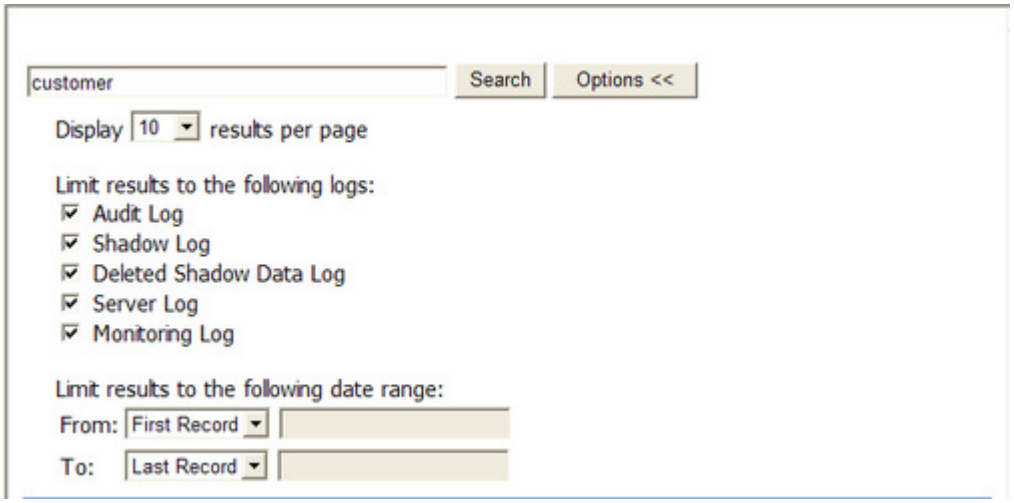

customer
Search
Options >>
Results 1 - 3 for customer.
1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View
1

La pagina dei risultati della ricerca è composta dalle seguenti sezioni:

- **Query di ricerca**: mostra i criteri di ricerca specificati.
- **Barra delle statistiche**: mostra il numero di risultati visualizzati nella pagina dei risultati della ricerca corrente.
- **Risultati della ricerca**: mostra un elenco numerato di voci con le informazioni che corrispondono ai criteri di ricerca specificati.
- **Esploratore risultati**: mostra il numero delle pagine di ricerca e consente di passare da una pagina all'altra.

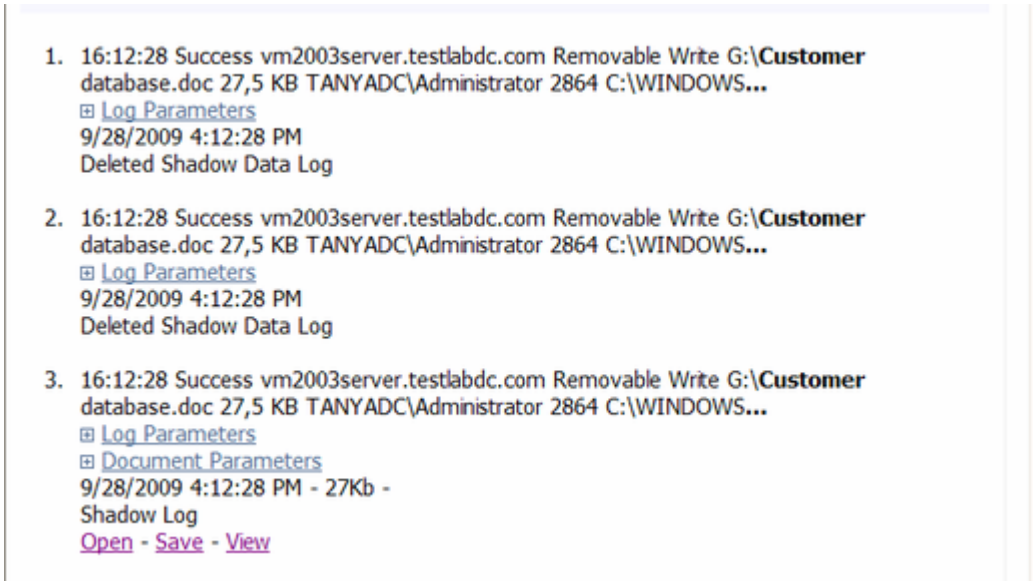
Queste sezioni vengono illustrate più nei dettagli di seguito.

Query di ricerca
Questa sezione si trova nella parte superiore della pagina dei risultati della ricerca. Fare clic su **Options** per visualizzare i criteri specificati per la ricerca.



Barra delle statistiche
Questa sezione si trova sopra l'area dei risultati della ricerca e ha l'aspetto seguente.

Risultati della ricerca
Questa sezione si trova sotto l'area della query di ricerca e la barra delle statistiche e ha l'aspetto seguente.


1. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
2. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
9/28/2009 4:12:28 PM
Deleted Shadow Data Log
3. 16:12:28 Success vm2003server.testlabdc.com Removable Write G:\Customer database.doc 27,5 KB TANYADC\Administrator 2864 C:\WINDOWS...
Log Parameters
Document Parameters
9/28/2009 4:12:28 PM - 27Kb -
Shadow Log
Open - Save - View

Un risultato della ricerca include i seguenti elementi:

- ***Frammenti***: porzioni di testo contenenti parole della query evidenziate (in grassetto). Questi frammenti consentono di visualizzare il contesto in cui sono state trovate le parole della query. Nella pagina dei risultati della ricerca sono visualizzati solo i primi tre frammenti per ogni risultato di ricerca.
- ***Log Parameters***: informazioni riassuntive recuperate dal registro per questo risultato della ricerca. Fare clic sul segno più (**+**) per espandere **Log Parameters** e visualizzare queste informazioni. Le informazioni cambiano a seconda del tipo di registro.

  Nota: se la voce di un registro ha un campo vuoto, questo campo non viene visualizzato in **Log Parameters**.

  Le seguenti informazioni vengono visualizzate nella sezione **Log Parameters** per un risultato recuperato dal registro Audit Log:

  - **Received Date/Time**: data e ora in cui l'evento è stato recuperato da DeviceLock Enterprise Server.
  - **Type**: classe dell'evento, **Success** in caso di accesso autorizzato e **Failure** in caso di accesso negato. Questo valore corrisponde a quello della colonna **Type** di Audit Log Viewer del server.
  - **Computer**: nome del computer da cui proviene l'Audit Log. Questo valore corrisponde a quello della colonna **Computer** di Audit Log Viewer del server.
  - **Date/Time**: data e ora in cui l'evento è stato recuperato da DeviceLock Service. Questo valore corrisponde a quello della colonna **Date/Time** di Audit Log Viewer del server.
  - **Source**:il tipo di periferica o protocollo coinvolto. Questo valore corrisponde a quello della colonna **Source** di Audit Log Viewer del server.

- **Action**: tipo di attività dell'utente. Questo valore corrisponde a quello della colonna **Action** di Audit Log Viewer del server.
- **Name**: nome dell'oggetto (file, periferica USB, ecc.) Questo valore corrisponde a quello della colonna **Name** di Audit Log Viewer del server.
- **Information**: altre informazioni relative alla periferica per l'evento, ad esempio flag di accesso, nomi di periferica, ecc. Questo valore corrisponde a quello della colonna **Information** di Audit Log Viewer del server.
- **User**: nome dell'utente associato a questo evento. Questo valore corrisponde a quello della colonna **User** di Audit Log Viewer del server.
- **PID**: codice identificativo del processo associato a questo evento. Questo valore corrisponde a quello della colonna **PID** di Audit Log Viewer del server.
- **Process**: percorso completo del file eseguibile del processo. In alcuni casi viene visualizzato il nome del processo e non il percorso. Questo valore corrisponde a quello della colonna **Process** di Audit Log Viewer del server.
- **Event**: numero identificativo del tipo di evento. Questo valore corrisponde a quello della colonna **Event** di Audit Log Viewer del server.

Le seguenti informazioni vengono visualizzate nella sezione **Log Parameters** per un risultato recuperato dal registro Shadow Log o Deleted Shadow Data:

- **Received Date/Time**: data e ora in cui i dati sono stati recuperati da DeviceLock Enterprise Server.
- **Status**: stato del record. Lo stato **Success** indica che i dati sono stati registrati correttamente, lo stato **Incomplete** indica che i dati non sono stati registrati completamente, mentre lo stato **Failed** viene associato alle copie shadow dei file la cui trasmissione è stata bloccata dalle regole basate sul contenuto (Content-Aware Rules). Questo valore corrisponde a quello della colonna **Status** di Shadow Log Viewer del server.
- **Computer** - nome del computer da cui proviene lo Shadow Log. Questo valore corrisponde a quello della colonna **Computer** di Shadow Log Viewer del server.
- **Date/Time**: data e ora in cui sono stati trasferiti i dati. Questo valore corrisponde a quello della colonna **Date/Time** di Shadow Log Viewer del server.
- **Source**:il tipo di periferica o protocollo coinvolto. Questo valore corrisponde a quello della colonna **Source** di Shadow Log Viewer del server.
- **Action**: tipo di attività dell'utente. Questo valore corrisponde a quello della colonna **Action** di Shadow Log Viewer del server.
- **File Name**: percorso originale del file o nome generato automaticamente dei dati che, inizialmente, non corrispondevano a un file (ad esempio immagini CD/DVD, immagini, dati scritti direttamente sul supporto o trasferiti tramite porte seriali/parallele). Questo valore corrisponde a quello della colonna **File Name** di Shadow Log Viewer del server.

- **File Size**: dimensione dei dati. Questo valore corrisponde a quello della colonna **File Size** di Shadow Log Viewer del server.
- **User**: nome dell'utente che ha trasferito i dati. Questo valore corrisponde a quello della colonna **User** di Shadow Log Viewer del server.
- **PID**: codice identificativo del processo utilizzato per trasferire i dati. Questo valore corrisponde a quello della colonna **PID** di Shadow Log Viewer del server.
- **Process**: percorso completo del file eseguibile del processo. In alcuni casi viene visualizzato il nome del processo e non il percorso. Questo valore corrisponde a quello della colonna **Process** di Shadow Log Viewer del server.

Le seguenti informazioni vengono visualizzate nella sezione **Log Parameters** per un risultato recuperato dal registro Server Log:

- **Type**: classe di evento, **Success**, **Information**, **Warning** o **Error**. Questo valore corrisponde a quello della colonna **Type** di Server Log Viewer.
- **Date/Time**: data e ora in cui si è verificato l'evento. Questo valore corrisponde a quello della colonna **Date/Time** di Server Log Viewer.
- **Event**: numero identificativo del tipo di evento. Questo valore corrisponde a quello della colonna **Event** di Server Log Viewer.
- **Information**: informazioni relative all'evento, ad esempio descrizioni di errori, avvisi, nomi e valori dei parametri modificati, ecc. Questo valore corrisponde a quello della colonna **Information** di Server Log Viewer.
- **Server**: nome del server su cui si è verificato l'evento. Questo valore corrisponde a quello della colonna **Server** di Server Log Viewer.
- **Record N**: numero del record. Questo valore corrisponde a quello della colonna **Record N** di Server Log Viewer.

Le seguenti informazioni vengono visualizzate nella sezione **Log Parameters** per un risultato recuperato dal registro Monitoring Log:

- **Type**: classe di evento, **Success**, **Information**, **Warning** o **Error**. Questo valore corrisponde a quello della colonna **Type** di Monitoring Log Viewer del server.
- **Date/Time**: data e ora in cui si è verificato l'evento. Questo valore corrisponde a quello della colonna **Date/Time** di Monitoring Log Viewer del server.
- **Event**: numero identificativo del tipo di evento. Questo valore corrisponde a quello della colonna **Event** di Monitoring Log Viewer del server.
- **Task Name**: nome dell'attività responsabile di questo evento. Può essere vuoto se l'evento non è collegato ad alcuna attività. Questo valore corrisponde a quello della colonna **Task Name** di Monitoring Log Viewer del server.
- **Computer Name**: nome del computer collegato all'attività responsabile di questo evento. Può essere vuoto se l'evento non è collegato ad alcun computer. Questo valore corrisponde a quello della colonna **Computer Name** di Monitoring Log Viewer del server.

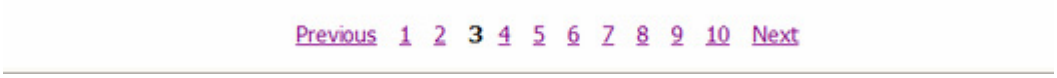
- **Information**: informazioni relative all'evento, ad esempio stati, errori, avvisi, ecc. Questo valore corrisponde a quello della colonna **Information** di Monitoring Log Viewer del server.
- **Server**: nome del server su cui si è verificato l'evento. Questo valore corrisponde a quello della colonna **Server** di Monitoring Log Viewer del server.
- **Record N**: numero del record. Questo valore corrisponde a quello della colonna **Record N** di Monitoring Log Viewer del server.

- ***Document Properties***: informazioni riassuntive recuperate dalle proprietà del documento per questo risultato della ricerca. Queste informazioni vengono recuperate casualmente e sono visualizzate solo per le copie shadow. Fare clic sul segno più (**+**) per espandere **Document Properties** e visualizzare queste informazioni. Le informazioni cambiano a seconda del tipo di file. Ad esempio, in **Document Properties** vengono visualizzate le seguenti informazioni per una copia shadow di un documento Word:
  - **Application**: Microsoft Office Word.
  - **Author**: nome dell'utente che ha creato il documento.
  - **Created**: data e ora di creazione del documento.
  - **LastSaved**: data e ora dell'ultimo salvataggio del documento.
  - **LastSavedBy**: nome dell'utente che ha eseguito l'ultimo salvataggio del documento.
  - **RevisionNumber**: numero di volte in cui il documento è stato salvato.
  - **Template**: nome del modello allegato al documento.
  - **Title**: nome del documento.
  - **TotalEditingTime**: numero di minuti durante i quali il documento è rimasto aperto per l'esecuzione di modifiche da quando è stato creato.
- ***La data e l'ora in cui è stata creata la voce di registro***.
- ***La dimensione della voce di registro***: questo valore viene visualizzato solo per le copie shadow recuperate da Shadow Log.
- ***Il nome del registro in cui sono state trovate le corrispondenze con la query***.
- ***Collegamenti Open, Save e View***: consente di accedere e gestire i risultati della ricerca (copie shadow) recuperati da Shadow Log. Per informazioni dettagliate su come gestire le copie shadow, consultare la sezione "Gestione dei risultati di ricerca recuperati da Shadow Log".

Nota: se la ricerca non produce alcun risultato, nella pagina dei risultati della ricerca viene visualizzato un messaggio che indica che non è stata trovata alcuna corrispondenza.

Esploratore risultati

Questa sezione si trova nella parte inferiore della pagina dei risultati della ricerca e ha l'aspetto seguente.



Per spostarsi avanti e indietro tra i risultati, fare clic su **Next** o **Previous** o selezionare un numero di pagina.

Gestione dei risultati di ricerca recuperati da Shadow Log

È possibile eseguire le seguenti operazioni sui risultati recuperati da Shadow Log:

- Aprire una copia shadow di un file nella sua applicazione nativa.
- Salvare una copia shadow di un file su qualsiasi percorso locale o di rete.
- Aprire e salvare una copia shadow di un file utilizzando il visualizzatore integrato.

Seguono le istruzioni dettagliate su come eseguire tali operazioni.

Per aprire una copia shadow di un file nella sua applicazione nativa

1. Eseguire la ricerca.
2. Nella pagina dei risultati della ricerca, fare clic su **Open** sotto il risultato della ricerca desiderato.

   La copia shadow del file viene aperta nella sua applicazione nativa.

   Se non è presente alcuna applicazione nativa, viene visualizzata la finestra di dialogo Apri con. Utilizzare questa finestra di dialogo per scegliere il programma con cui aprire il file.

   Se viene aperta una copia shadow di un file acquisito dai tipi di periferica stampante o porta parallela, la copia viene sempre aperta nel DeviceLock Printer Viewer integrato.

   DeviceLock Printer Viewer consente di visualizzare un documento shadow stampato nel formato di spooler di stampa, di inviarlo nuovamente alla stampante e di salvarlo in formato grafico (BMP, GIF, JPEG, PNG, EMF o TIFF). Sono supportati i seguenti formati di spooler di stampa: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, stampa GDI (ZjStream) ed EMF Spooled File.

Per salvare una copia shadow di un file su qualsiasi percorso locale o di rete

1. Eseguire la ricerca.
2. Nella pagina dei risultati della ricerca, fare clic su **Save** sotto il risultati della ricerca desiderato.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

3. Nella casella **Save in** della finestra di dialogo **Save As**, selezionare la posizione in cui salvare la copia shadow.
4. Nella casella **File name**, digitare il nome di file desiderato.

5. Fare clic su **Save**.

   Se i dati sono stati trasferiti da un utente sotto forma di file, vengono memorizzati in Shadow Log e possono essere salvati sotto forma di file anche sul computer locale.

   Quando l'utente scrive i dati su un disco CD/DVD, tutti i dati vengono memorizzati in Shadow Log come immagine CD/DVD singola (un'immagine per ogni disco/sessione CD/DVD scritto/a) in formato CUE.

   Le immagini CD/DVD e gli altri dati che non sono stati trasferiti inizialmente sotto forma di file (accesso diretto accesso periferica o trasferimento tramite porta seriale/parallela) presentano dei nomi di file generati automaticamente in base al tipo di azione, alla lettera dell'unità, al nome del dispositivo e alla data/ora (ad esempio direct_write(E:) 19:18:29 17.07.2006.bin).

   Ciascuna immagine CD/DVD viene salvata sul computer locale sotto forma di due file: il file dei dati con estensione .bin (ad esempio direct_write(E_) 19_18_29 17_07_2006.bin) e il file di elenco tracce che ha lo stesso nome del file dei dati e l'estensione .cue (ad esempio direct_write(E_) 19_18_29 17_07_2006_bin.cue). Entrambi i file sono necessari per aprire l'immagine CD/DVD nell'applicazione esterna che supporta il formato CUE (ad esempio Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO e tanti altri ancora).

Per aprire e salvare una copia shadow di un file utilizzando il visualizzatore integrato

1. Eseguire la ricerca.
2. Nella pagina dei risultati della ricerca, fare clic su **View** sotto il risultato della ricerca desiderato.

   La copia shadow si apre nel visualizzatore integrato.

3. Nel visualizzatore integrato, fare clic su una qualsiasi delle opzioni di visualizzazione seguenti:

   - **Hex**: mostra i dati in formato hex e sotto forma di parole.
   - **Autodetect Text**: attiva il rilevamento automatico della codifica per il testo e mostra i dati unicamente in formato testo.
   - **ANSI Text**: specifica la codifica ANSI per il testo e mostra i dati unicamente in formato testo.
   - **UTF-16 Text**: specifica la codifica Unicode UTF-16 per il testo e mostra i dati unicamente in formato testo.
   - **UTF-16BE Text**: specifica la codifica Unicode UTF-16 (Big Endian) per il testo e mostra i dati unicamente in formato testo.

   Per salvare il file, fare clic su **Save**. Nella finestra di dialogo **Save As** visualizzata, attenersi alle seguenti istruzioni:

   - Nella finestra di dialogo **Save As**, selezionare la posizione in cui salvare il file.
   - Nella casella **File name**, digitare il nome di file desiderato.
   - Fare clic su **Save**.

4. Fare clic su **Close** per chiudere il visualizzatore.

Gestione mediante i Criteri di gruppo

Informazioni generali

Sebbene sia possibile utilizzare la console di gestione di DeviceLock per gestire le autorizzazioni di DeviceLock, quest'ultimo fornisce un meccanismo più potente per modificare le impostazioni e assegnare le autorizzazioni in un dominio di Active Directory: i Criteri di gruppo. In un ambiente di rete, gli amministratori di sistema possono utilizzare i criteri per controllare le impostazioni di DeviceLock da una singola stazione, indipendentemente dalle dimensioni della rete.

In un ambiente Active Directory, i Criteri di gruppo consentono di eseguire attività di amministrazione basate su criteri. Mediante l'utilizzo dei servizi directory e dei gruppi di protezione, i Criteri di gruppo forniscono flessibilità e supporto alle informazioni di configurazione. Le impostazioni relative ai criteri vengono create tramite lo snap-in Microsoft Management Console (MMC).

Una delle funzionalità più importanti di DeviceLock è l'integrazione con Active Directory, che consente agli amministratori di sistema di gestire in maniera più semplice e conveniente le autorizzazioni di DeviceLock nelle reti di grandi dimensioni.

L'integrazione con Active Directory elimina la necessità di installare applicazioni di terze parti per la gestione e la distribuzione centralizzata. DeviceLock non necessita di una versione basata su server per controllare la rete, ma utilizza le funzioni standard fornite da Active Directory.

Tramite i Criteri di gruppo è possibile:

- Installare DeviceLock Service su tutti i computer della rete, inclusi quelli che non sono correntemente avviati o che sono stati appena collegati alla rete.
  Per ulteriori informazioni sulla distribuzione di DeviceLock Service, leggere la sezione Installazione tramite Criteri di gruppo.

- Controllare e configurare simultaneamente DeviceLock Service su un numero elevato di computer appartenenti a domini/unità organizzative differenti.
  Le impostazioni predefinite di DeviceLock vengono distribuite automaticamente anche ai computer correntemente non avviati o che sono stati appena collegati alla rete.

- Ottenere informazioni in merito ai criteri in fase corrente di applicazione e prevedere gli effetti di eventuali modifiche alle impostazioni dei criteri.
  Per ulteriori informazioni, leggere la sezione Utilizzare Gruppo di criteri risultante (RSoP).

Nota: per gestire DeviceLock mediante i Criteri di gruppo, è necessario che Active Directory sia correttamente installato e configurato. Per maggiori informazioni relative all'installazione e alla configurazione di Active Directory, fare riferimento alla documentazione fornita da Microsoft.

Applicare i Criteri di gruppo

I criteri vengono applicati all'avvio della macchina. Quando un utente accende il computer, il sistema applica i criteri di DeviceLock.

Se necessario, è possibile riapplicare i criteri su base periodica. Per impostazione predefinita, i criteri vengono applicati ogni 90 minuti. Per impostare un intervallo di tempo differente, utilizzare Editor oggetti Criteri di gruppo. Per ulteriori informazioni, leggere la seguente Knowledge Base di Microsoft: http://support.microsoft.com/kb/203607/it.

I criteri possono essere riapplicati anche su richiesta. Per aggiornare immediatamente le impostazioni dei criteri correnti in ambiente Windows XP o versione successiva, gli amministratori possono eseguire da riga di comando l'utility di Microsoft ***gpupdate.exe /force***. Se si utilizza Windows 2000, gli amministratori possono eseguire da riga di comando l'utility di Microsoft ***secedit /refreshpolicy machine_policy /enforce***.

Quando si applicano i criteri, il sistema interroga il servizio directory per ottenere l'elenco degli oggetti Criteri di gruppo (GPO) da elaborare. Ciascun GPO è associato ad un contenitore Active Directory a cui appartengono il computer o l'utente. Per impostazione predefinita, il sistema applica i GPO nel seguente ordine: a livello di computer locale, a livello di sito, a livello di dominio e a livello di unità organizzativa. Quindi, al computer vengono applicate le impostazioni relative ai criteri dell'ultimo contenitore Active Directory elaborato.

Durante l'elaborazione del GPO, il sistema verifica l'elenco di controllo di accesso (ACL) associato al GPO. Se una voce di controllo di accesso (ACE) blocca l'accesso del computer al GPO, il sistema non applica le impostazioni relative ai criteri del GPO. Se invece ACE concede l'accesso al GPO, il sistema applica le impostazioni relative ai criteri del GPO.

Regole di ereditarietà standard GPO

Le impostazioni dei criteri non configurate in un GPO possono essere ignorate poiché non vengono ereditate dal contenitore figlio; vengono ereditate solo le impostazioni dei criteri che sono state configurate. Sono possibili tre scenari:

- L'impostazione di un criterio viene configurata per un padre ma non per un figlio.
- L'impostazione di un criterio applicata ad un padre è compatibile con la stessa impostazione applicata ad un figlio.
- L'impostazione di un criterio configurata per un padre non è compatibile con la stessa impostazione configurata per un figlio.

Se l'impostazione di un criterio viene configurata per un'unità organizzativa padre ma non per un'unità organizzativa figlio, quest'ultima erediterà l'impostazione del criterio dal contenitore padre.

Se l'impostazione di un criterio configurata per un'unità organizzativa padre è compatibile con l'impostazione configurata per un'unità organizzativa figlio, quest'ultima verrà applicata ed erediterà anche l'impostazione del contenitore padre.

Se l'impostazione di un criterio configurata per un'unità organizzativa padre non è compatibile con la stessa impostazione in un GPO differente configurata per un'unità organizzativa figlio, l'unità organizzativa figlio non erediterà l'impostazione GPO del contenitore padre. Verrà applicata l'impostazione dell'unità organizzativa figlio, tranne che in un caso.

Se l'impostazione di un criterio configurata per un'unità organizzativa padre viene disattivata e l'unità organizzativa figlio modifica la stessa impostazione, la modifica dell'unità organizzativa figlio non viene applicata.

Avviare DeviceLock Group Policy Manager

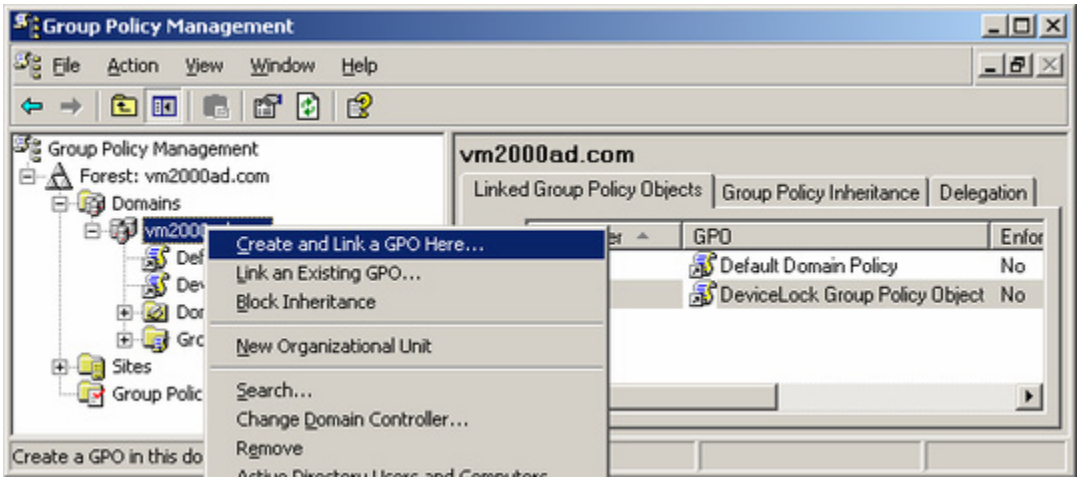
Il gestore dei Criteri di gruppo di DeviceLock si integra con l'editor degli oggetti Criteri di gruppo (GPO). Per utilizzare il gestore dei Criteri di gruppo di DeviceLock sul PC locale piuttosto che sul controller di dominio, è necessario che l'editor degli oggetti Criteri di gruppo sia installato localmente. Si consiglia di installare la console Gestione Criteri di gruppo (GPMC), scaricabile dal sito Web di Microsoft.

Per aprire il gestore dei Criteri di gruppo di DeviceLock, avviare Editor oggetti Criteri di gruppo (GPO):

1. Avviare lo snap-in Gestione Criteri di gruppo.

   Se lo snap-in Gestione Criteri di gruppo non è installato sul proprio computer, è possibile usare lo snap-in Utenti e computer di Active Directory.

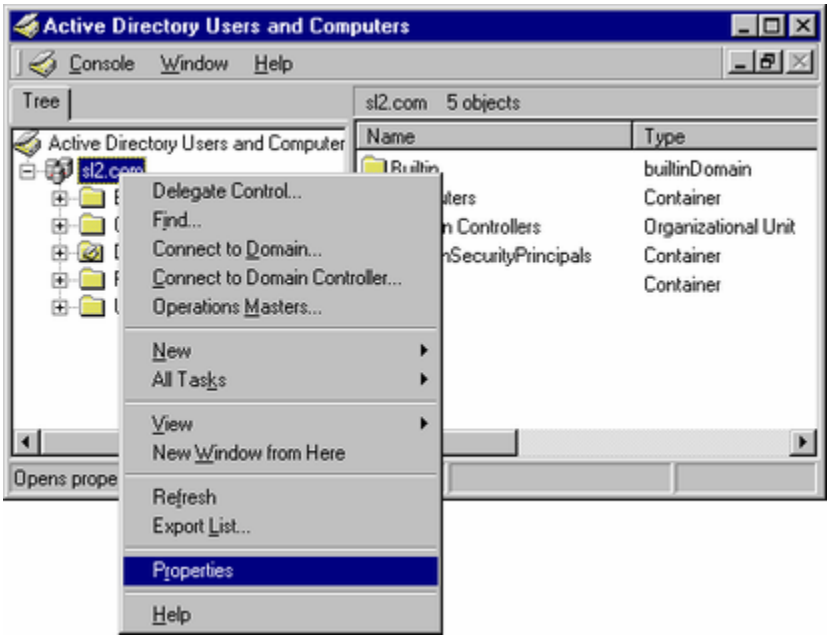
2. Nella struttura ad albero, selezionare il dominio.



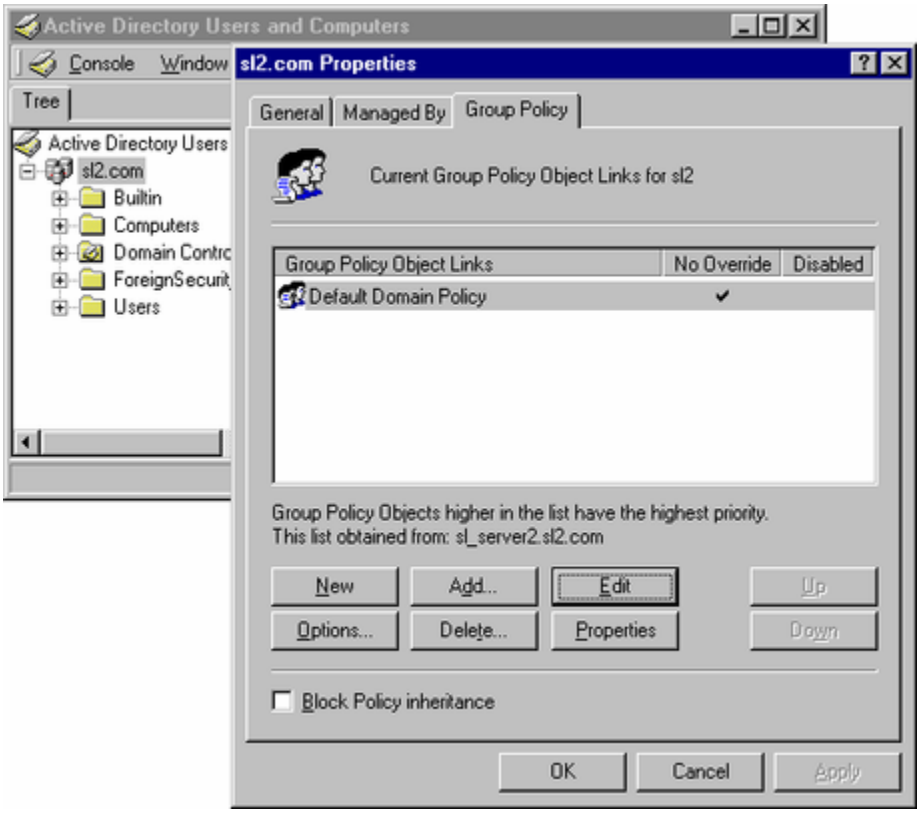
3. Selezionare l'oggetto Criteri di gruppo desiderato e quindi selezionare **Edit** dal menu contestuale richiamabile con il pulsante destro del mouse. Per creare un nuovo

oggetto Criteri di gruppo, selezionare **Create and Link a GPO Here** dal menu contestuale del dominio.

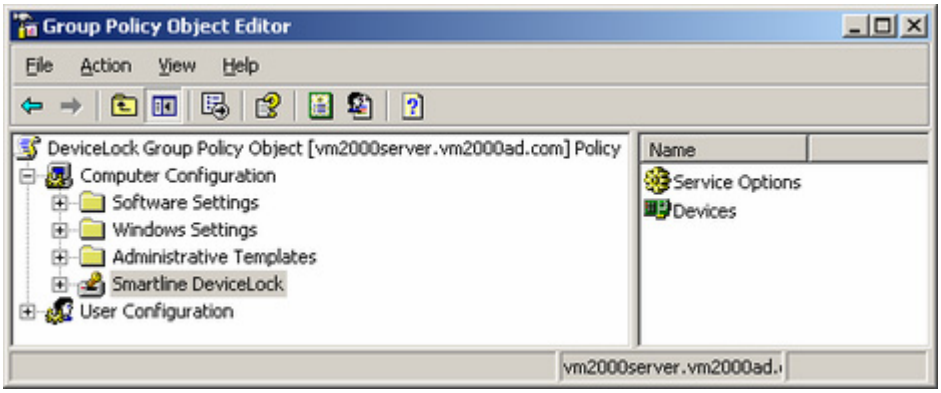
Se si utilizza lo snap-in Utenti e computer di Active Directory, fare clic con il pulsante destro del mouse e quindi scegliere **Properties**.



Fare clic sulla scheda **Criteri di gruppo**, selezionare l'oggetto Criteri di gruppo desiderato e fare clic sul pulsante **Modifica**. Per creare un nuovo criterio di gruppo, fare clic su **Aggiungi**.

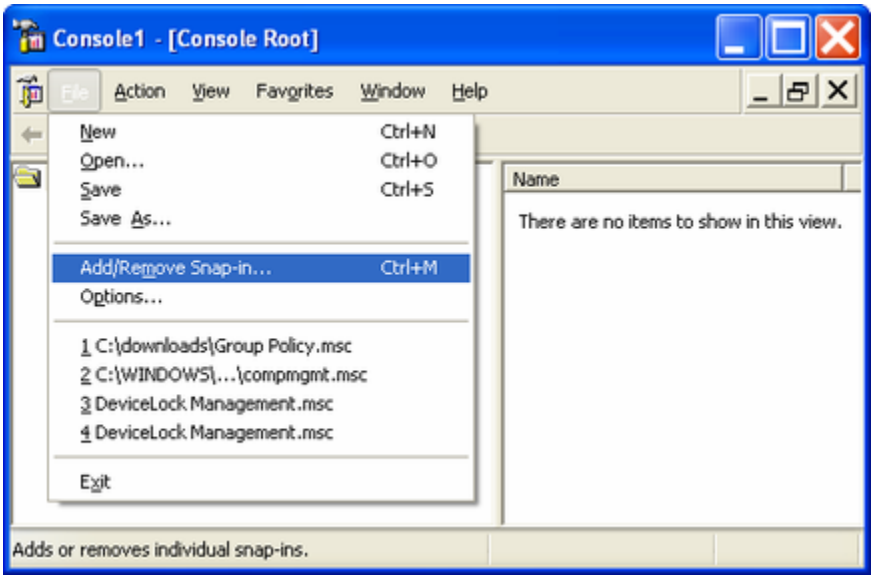


4. Attendere l'avvio di Editor oggetti Criteri di gruppo. L'operazione potrebbe richiedere alcuni secondi.
5. Selezionare **DeviceLock** in **Configurazione computer**.

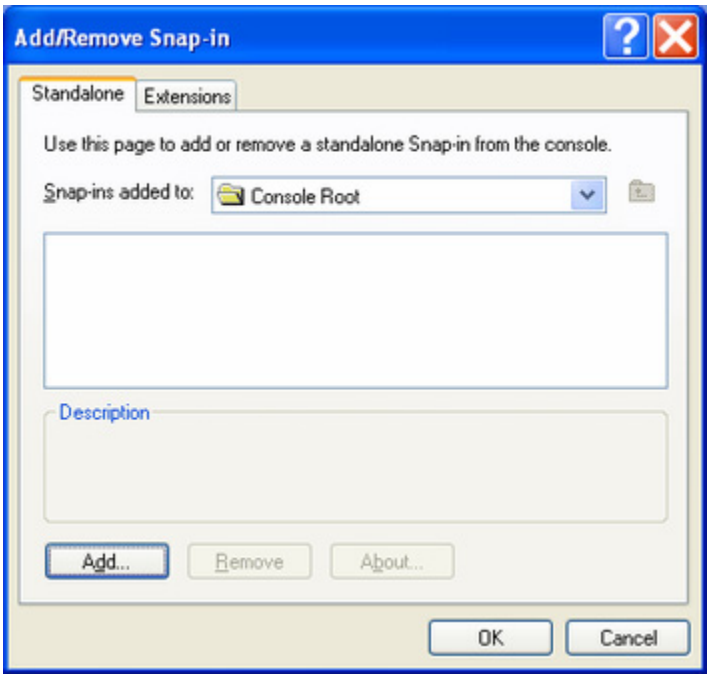


In alternativa, per avviare Editor oggetti Criteri di gruppo, eseguire MMC e aggiungere manualmente lo snap-in Editor oggetti Criteri di gruppo:

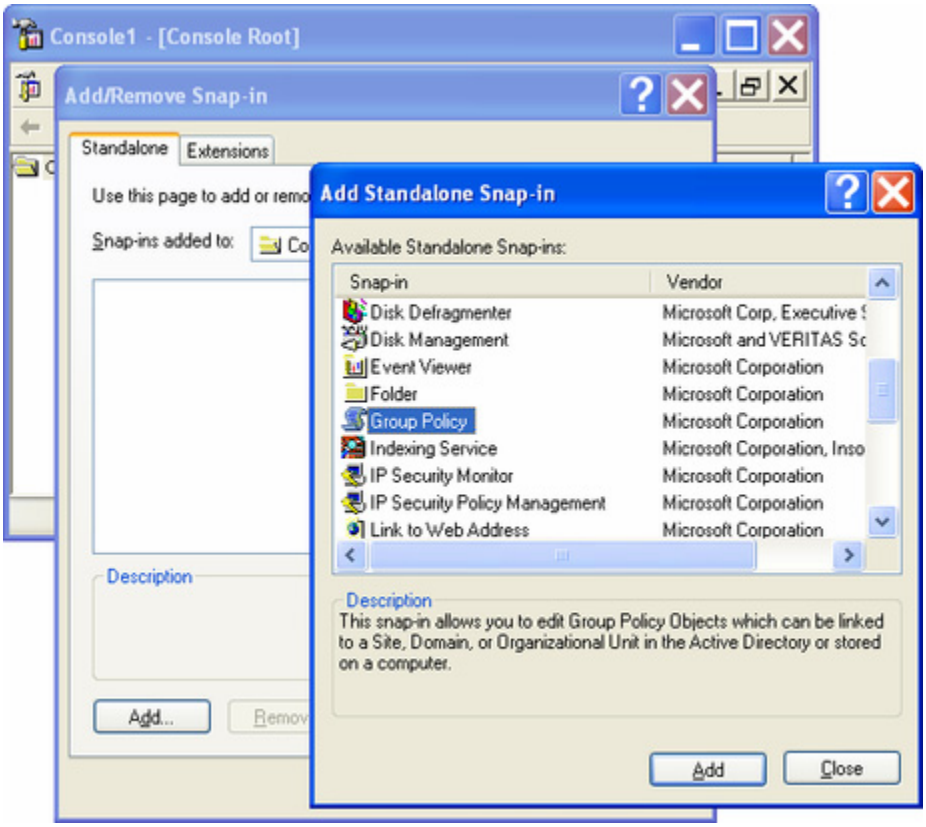
1. Avviare **mmc** dalla riga di comando o dal menu **Esegui**.
2. Selezionare **Aggiungi/Rimuovi snap-in** dal menu **File**.



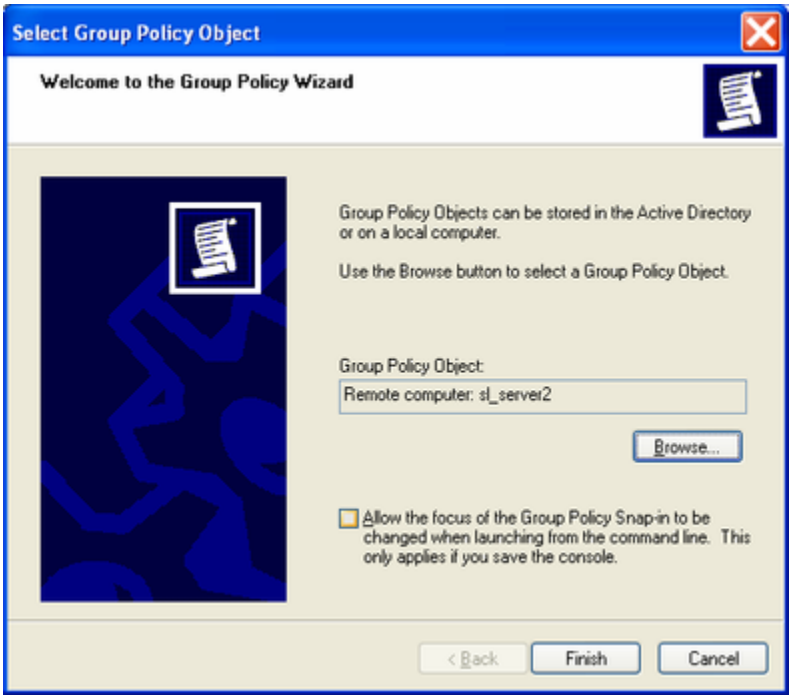
3. Selezionare la scheda **Autonomo** e quindi fare clic sul pulsante **Aggiungi**.



4. Selezionare **Editor oggetti Criteri di gruppo** dall'elenco, quindi scegliere **Aggiungi**.



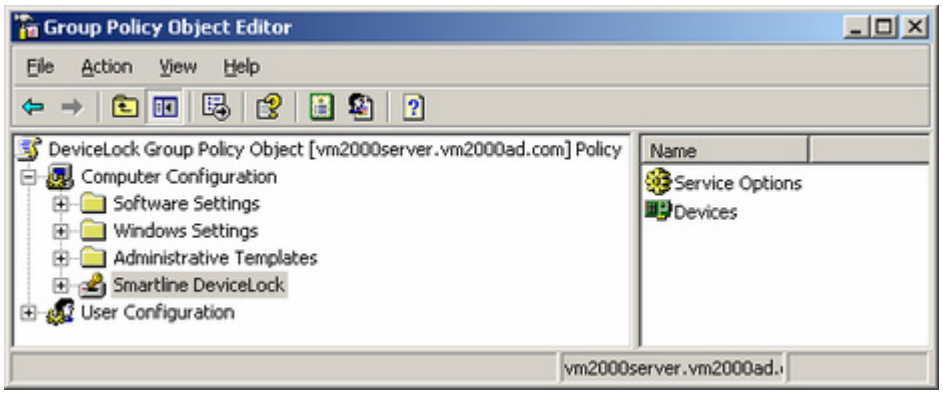
5. Selezionare un oggetto Criteri di gruppo da Active Directory o un computer locale, quindi fare clic su **Fine**.


Select Group Policy Object
Welcome to the Group Policy Wizard
Group Policy Objects can be stored in the Active Directory or on a local computer.
Use the Browse button to select a Group Policy Object.
Group Policy Object:
Remote computer: sl_server2
Browse...
Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel

6. Fare clic sul pulsante **Chiudi** per chiudere la finestra **Aggiungi snap-in autonomo**.
7. Fare clic su **OK** per aggiungere lo snap-in.
8. Espandere **Configurazione computer** e selezionare **DeviceLock**.

Utilizzare DeviceLock Group Policy Manager

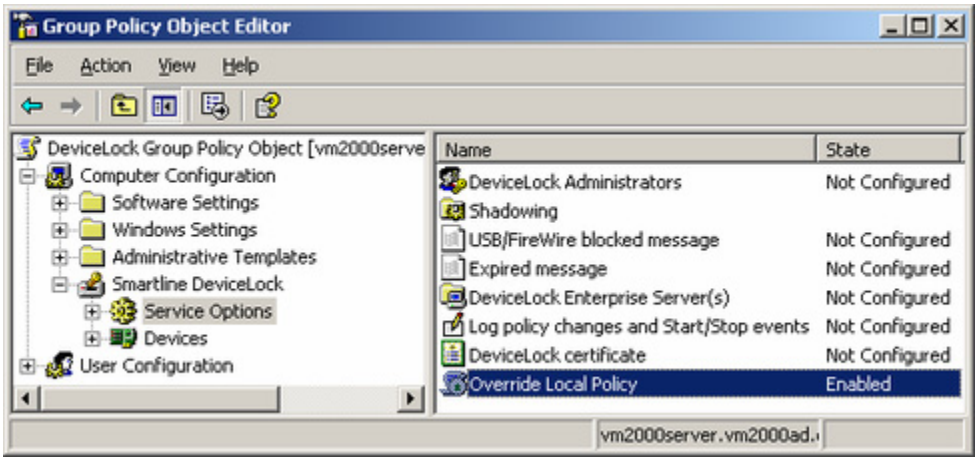
Non esistono sostanziali differenze tra la procedura di gestione di DeviceLock Service tramite DeviceLock Management Console e tramite DeviceLock Group Policy Manager. Per ulteriori informazioni, leggere la sezione Gestione di DeviceLock Service.



Non è possibile gestire DeviceLock Enterprise Server e visualizzare i registri eventi di controllo e di shadowing con DeviceLock Group Policy Manager. Per tali operazioni, utilizzare DeviceLock Management Console.

La gestione di DeviceLock Service tramite DeviceLock Group Policy Manager include quattro funzionalità aggiuntive rispetto a DeviceLock Management Console:

1. **Override Local Policy** – per impedire la modifica delle autorizzazioni e delle regole di controllo definite per i computer client (senza utilizzare Editor oggetti Criteri di gruppo), selezionare **Override Local Policy** in **Service Options**. Ciò consente di attivare la modalità Criteri di gruppo per tutti i computer in GPO, impedendo l'attivazione della modalità Local Policy.



Se il parametro Override Local Policy è attivato, non sarà possibile disattivare il parametro Use Group Policy (in Service Options) di DeviceLock Management Console e DeviceLock Enterprise Manager.

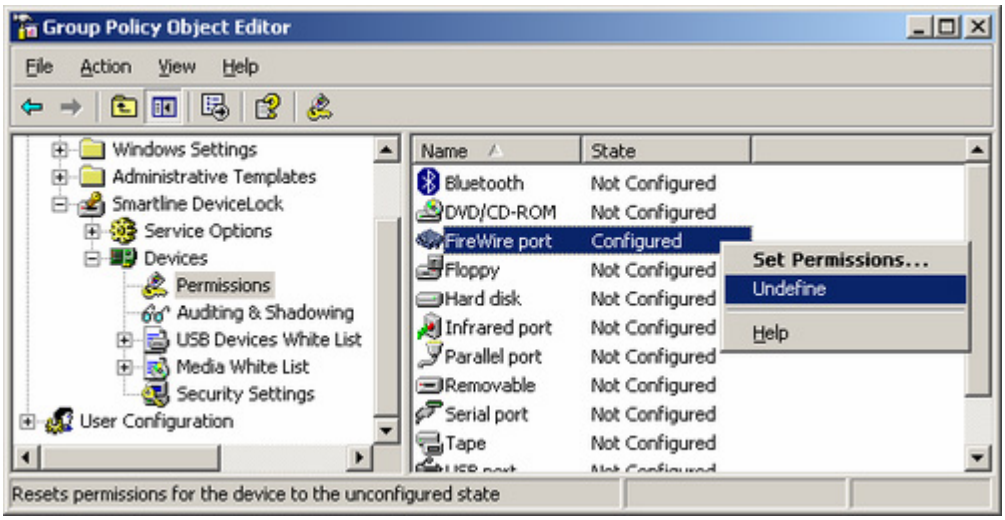
La tabella seguente mostra l'effetto delle diverse impostazioni dei parametri **Use Group Policy** e **Override Local Policy** sulla modalità di applicazione dei criteri:

MODALITÀ DI APPLICAZIONE DEI CRITERI	USE GROUP POLICY	OVERRIDE LOCAL POLICY
Applicazione dei soli criteri locali.	Disattivato	Disattivato
Applicazione dei soli criteri di gruppo.	Attivato	Attivato
Applicazione dei criteri locali fino alla replica di Active Directory.	Attivato	Disattivato

Durante l'impostazione del parametro **Override Local Policy**, considerare quanto segue:

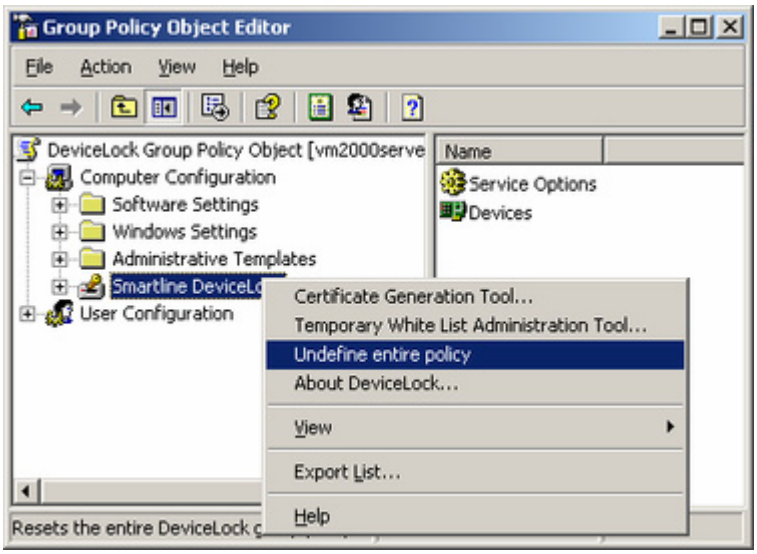
- La disattivazione del parametro **Override Local Policy** non annulla la replica di Active Directory.
- Quando si disattiva il parametro **Override Local Policy**, tutte le impostazioni di DeviceLock Service configurate tramite DeviceLock Management Console e DeviceLock Enterprise Manager risultano immediatamente effettive.

2. **Undefine** – consente di reimpostare tutti i parametri (stato non definito). Tutti i parametri non definiti vengono ignorati in questo GPO. Per ulteriori informazioni, leggere la sezione Regole di ereditarietà standard GPO.

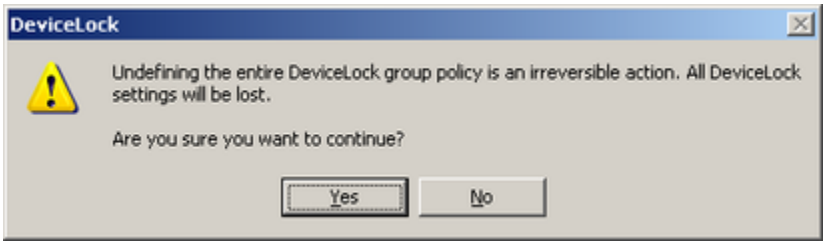


Per reimpostare un parametro (stato non definito), fare clic su di esso con il pulsante destro del mouse e scegliere **Undefine** dal menu sensibile al contesto. È possibile reimpostare alcuni parametri rendendo grigia la relativa casella di controllo.

3. **Undefine entire policy** – consente di reimpostare tutti i parametri (stato non definito) con un solo clic. Equivale a reimpostare manualmente ciascun parametro (vedere opzione precedente).



Per reimpostare tutti i parametri sullo stato "non definito", scegliere **Undefine** entire policy dal menu sensibile al contesto dell'oggetto principale di DeviceLock.


DeviceLock
Undefining the entire DeviceLock group policy is an irreversible action. All DeviceLock settings will be lost.
Are you sure you want to continue?
Yes
No

4. **Remove Offline** - È possibile rimuovere qualsiasi impostazione di criteri (autorizzazioni, regole di controllo e di shadowing, liste bianche, ecc.), sia per le periferiche sia per i protocolli, al fine di applicare criteri regolari in questo GPO (Group Policy Object: Oggetto criteri di gruppo). Per farlo, fare clic con il pulsante destro del mouse su qualsiasi impostazione di criterio, quindi scegliere **Remove Offline**.

Nota: per gestire DeviceLock Service mediante i Criteri di gruppo, è necessario installare e avviare DeviceLock Service su tutti i computer appartenenti al GPO. Per maggiori informazioni sull'installazione del servizio, consultare la sezione Distribuzione di DeviceLock Service.

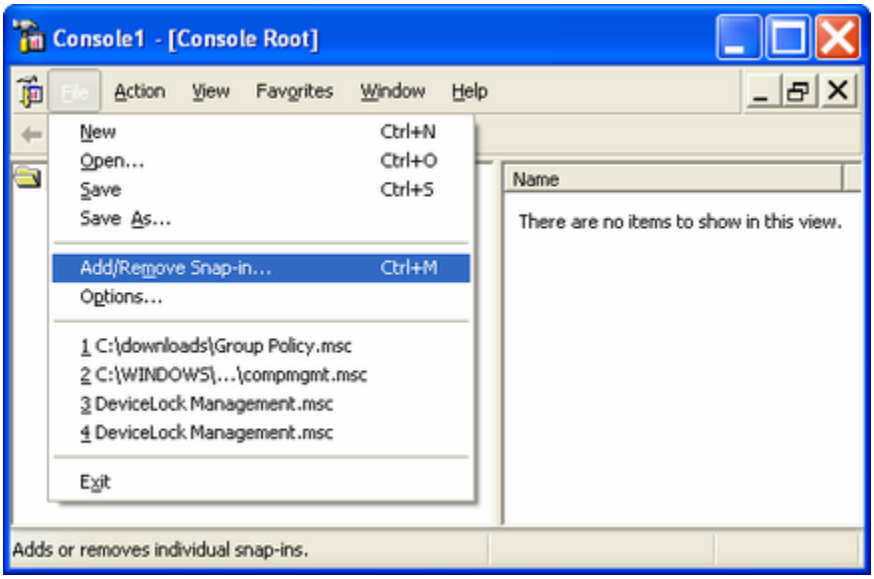
Inoltre, poiché i Criteri di gruppo vengono riapplicati su base periodica (per impostazione predefinita, ogni 90 minuti), le modifiche non hanno effetto immediato. Per ulteriori informazioni, consultare la sezione Applicare i Criteri di gruppo.

Utilizzare Gruppo di criteri risultante (RSoP)

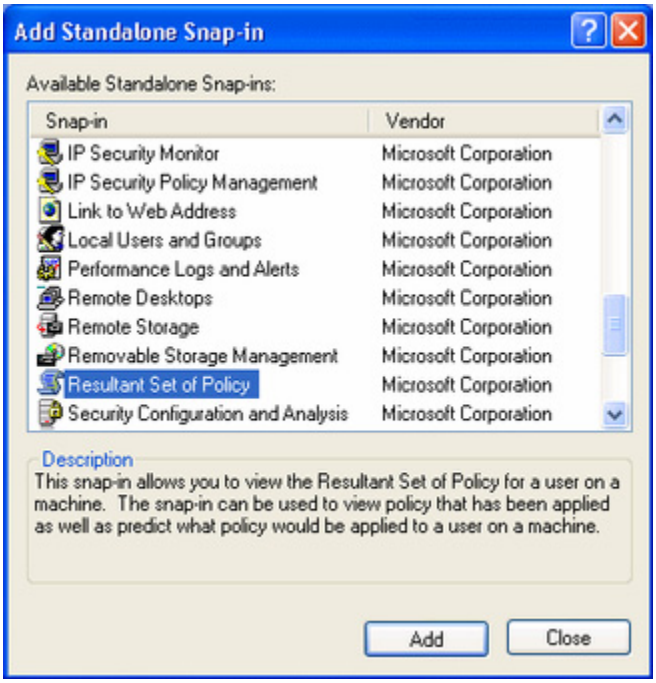
DeviceLock supporta lo snap-in Gruppo di criteri risultante. Grazie a questo snap-in standard di Windows, è possibile ottenere informazioni in merito a tutte le impostazioni dei criteri di DeviceLock e prevedere gli effetti di eventuali modifiche alle impostazioni dei criteri applicati ad un determinato computer.

Per utilizzare RSoP, eseguire MMC e aggiungere manualmente lo snap-in Gruppo di criteri risultante:

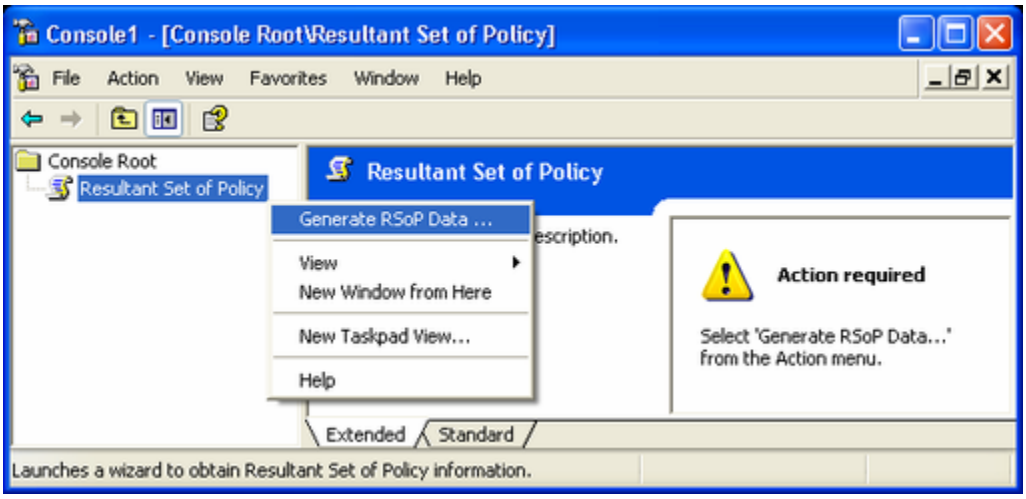
1. Avviare **mmc** dalla riga di comando o dal menu **Esegui**.
2. Selezionare **Aggiungi/Rimuovi snap-in** dal menu **File**.



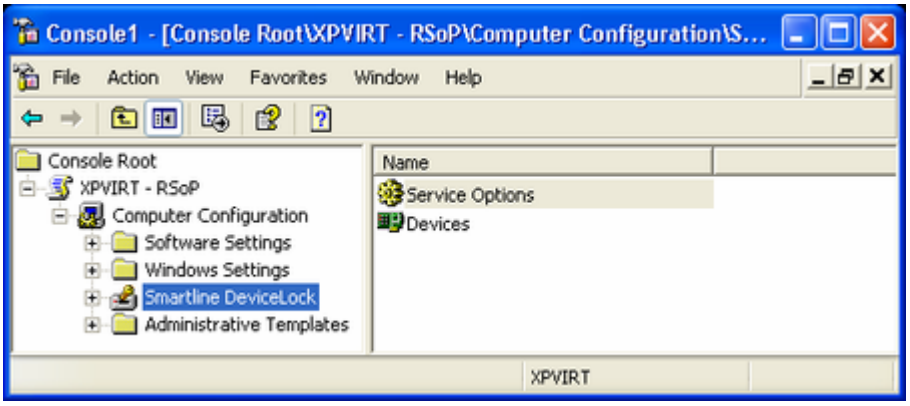
3. Selezionare la scheda **Autonomo** e quindi fare clic sul pulsante **Aggiungi**.
4. Selezionare **Criteri di gruppo risultante** dall'elenco, quindi scegliere **Aggiungi**.


Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Vendor
IP Security Monitor Microsoft Corporation
IP Security Policy Management Microsoft Corporation
Link to Web Address Microsoft Corporation
Local Users and Groups Microsoft Corporation
Performance Logs and Alerts Microsoft Corporation
Remote Desktops Microsoft Corporation
Remote Storage Microsoft Corporation
Removable Storage Management Microsoft Corporation
Resultant Set of Policy Microsoft Corporation
Security Configuration and Analysis Microsoft Corporation
Description
This snap-in allows you to view the Resultant Set of Policy for a user on a machine. The snap-in can be used to view policy that has been applied as well as predict what policy would be applied to a user on a machine.
Add
Close

5. Fare clic sul pulsante **Chiudi** per chiudere la finestra **Aggiungi snap-in autonomo**.
6. Nella struttura ad albero della console, selezionare **Criteri di gruppo risultante**.



7. Selezionare **Genera dati RSoP** dal menu sensibile al contesto richiamabile facendo clic con il pulsante destro del mouse.
8. Completare la Ricerca guidata gruppo di criteri risultante per ottenere informazioni RSoP dal computer selezionato.
9. Espandere **Configurazione computer** e selezionare **DeviceLock**.



Non è possibile utilizzare RSoP per modificare i criteri – tutti i parametri sono in sola lettura.

RSoP è particolarmente utile per conoscere quale GPO sta per essere applicato ad un computer.

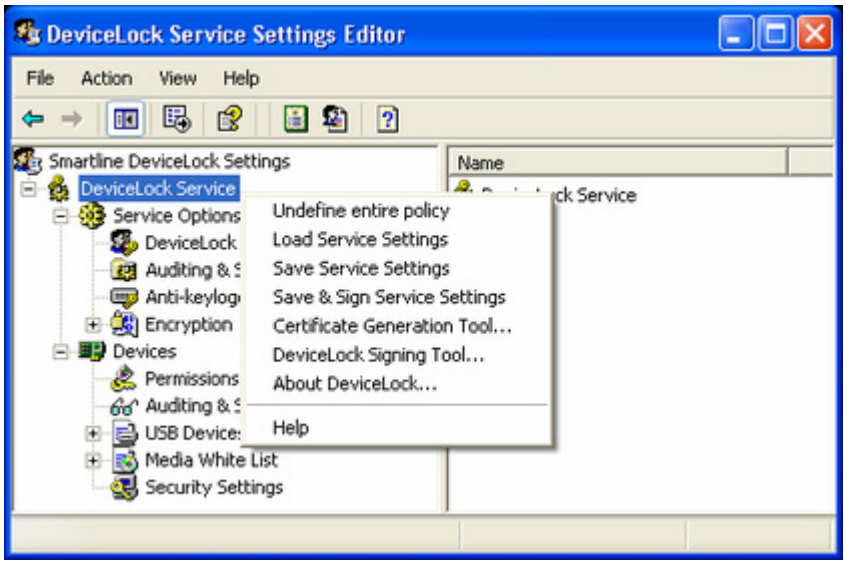
Per ulteriori informazioni su Gruppo di criteri risultante, leggere il seguente articolo in linea di Microsoft: http://technet.microsoft.com/it-it/library/cc775741(WS.10).aspx.

DeviceLock Service Settings Editor

Informazioni generali

DeviceLock Service Settings Editor è utilizzato per creare e modificare file XML esterni introducendo impostazioni, autorizzazioni, regole di controllo e di shadowing per DeviceLock Service.

DeviceLock Service Settings Editor si installa unitamente alle altre console di gestione.



Le procedure di definizione dei criteri tramite DeviceLock Management Console e DeviceLock Service Settings Editor sono molto simili. Per ulteriori informazioni, consultare la sezione Gestione di DeviceLock Service di questo manuale.

A differenza di DeviceLock Management Console, in DeviceLock Service Settings Editor:

- Non è necessario connettersi a un computer dotato di DeviceLock Service. DeviceLock Service Settings Editor modifica e archivia le impostazioni in file XML esterni e consente la creazione/modifica non in linea dei criteri. Funziona in maniera simile a DeviceLock Group Policy Manager ma utilizza file XML anziché gli oggetti Criteri di gruppo (GPO).
- È possibile reimpostare qualsiasi parametro (o tutti i parametri contemporaneamente) nello stato non configurato. I parametri non definiti sono ignorati all'atto dell'applicazione del criterio a DeviceLock Service.
- È possibile rimuovere qualsiasi impostazione di criteri (autorizzazioni, regole di controllo e di shadowing, liste bianche, ecc.), sia per le periferiche sia per i protocolli, al fine di applicare criteri regolari in questo file di criteri.

Per creare un criterio completamente nuovo è sufficiente eseguire DeviceLock Service Settings Editor e iniziare ad apportare modifiche al criterio predefinito (vuoto).

Per modificare un criterio esistente, caricare il file XML corrispondente in DeviceLock Service Settings Editor utilizzando la voce **Load Service Settings** del menu contestuale e apportare quindi le modifiche desiderate.

Se si crea un nuovo criterio da zero, selezionare **Save Service Settings** nel menu contestuale per salvarlo in un file XML. In alternativa, è possibile utilizzare il comando **Save & Sign Service Settings** del menu contestuale per salvare il criterio in un file XML esterno e firmarlo automaticamente utilizzando il certificato di DeviceLock (la chiave privata) più recente. La voce di menu **Save & Sign Service Setting**s è disattivata se DeviceLock Signing Tool non dispone di una chiave privata caricata in precedenza.

In seguito i file dei criteri creati utilizzando DeviceLock Service Settings Editor possono essere caricati mediante DeviceLock Management Console e/o DeviceLock Group Policy Manager.

Inoltre, è possibile inviare i file dei criteri agli utenti che utilizzano computer non in linea (irraggiungibili dalle console di gestione). Per evitarne la modifica non autorizzata, è opportuno firmare tali file utilizzando il certificato di DeviceLock (la chiave privata) mediante DeviceLock Signing Tool. Per ulteriori informazioni, consultare la sezione Impostazioni del servizio di questo manuale.

Se si modifica un file di criteri esistente, DeviceLock Service Settings Editor salva automaticamente le modifiche.

Nota: solo le impostazioni espressamente definite in un file di criteri vengono applicate ai computer client. Tutte le impostazioni di criteri con lo stato **Not Configured** vengono ignorate dai computer client.

DeviceLock Service Settings Editor è utilizzato inoltre nel plug-in Set Service Settings di DeviceLock Enterprise Manager. Questo plug-in esegue DeviceLock Service Settings Editor come applicazione esterna avviandola con il file XML selezionato nella finestra di dialogo delle impostazioni del plug-in.

Se si apportano modifiche al criterio (modifica dei parametri, impostazione delle autorizzazioni, definizione delle white list, ecc.) nel file XML inoltrato dal plug-in all'editor, DeviceLock Service Settings Editor le salva automaticamente in tale file. Una volta completata la modifica del criterio, è sufficiente uscire da DeviceLock Service Settings Editor e tornare alla finestra di dialogo delle impostazioni del plug-in.

Per ulteriori informazioni, consultare la sezione Set Service Settings di questo manuale.

DeviceLock Enterprise Manager

Informazioni generali

DeviceLock Enterprise Manager consente di visualizzare e modificare i criteri di protezione definiti per i tipi di periferica e per i protocolli, di installare, aggiornare e disinstallare DeviceLock Service e di visualizzare i registri di controllo e shadowing per tutti i computer presenti in una rete di grandi dimensioni. Se la rete non dispone del servizio di directory Microsoft Active Directory, si consiglia di utilizzare DeviceLock Enterprise Manager.

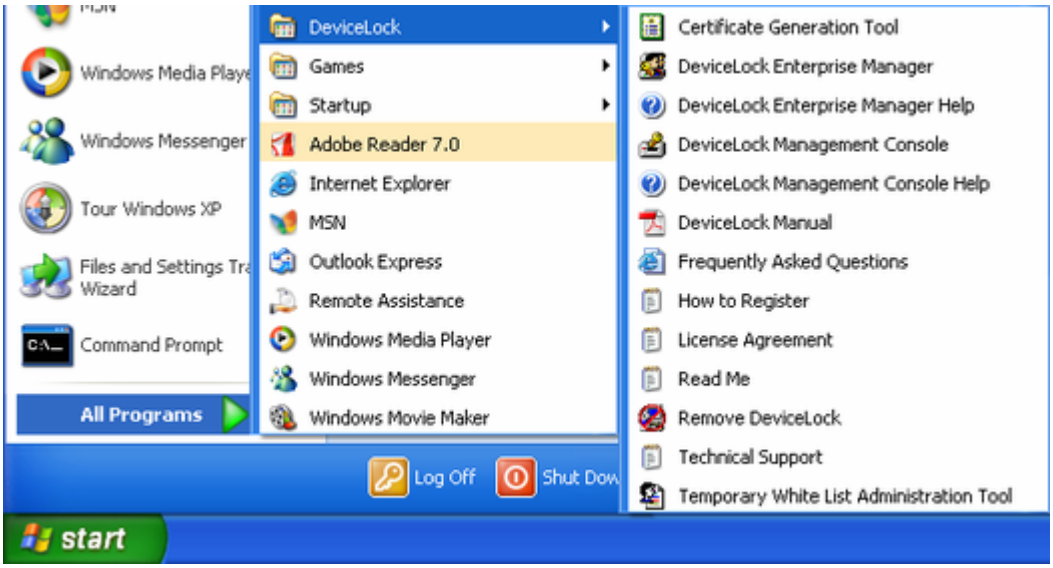
Basato su tecnologia multithread, questa console consente di eseguire più velocemente tutte le attività necessarie per gestire i computer connessi in una rete di grandi dimensioni.

DeviceLock Enterprise Manager memorizza, confronta e filtra i dati ricevuti da tutti i computer. Gli amministratori di rete possono creare delle "istantanee" dei propri sistemi per futuri confronti e per identificare le modifiche apportate.

DeviceLock Enterprise Manager è basato su di una flessibile architettura a plug-in che consente di utilizzare i moduli in base alle proprie esigenze. Ciascun modulo (plug-in) esegue un'operazione e visualizza le informazioni raccolte in una propria finestra.

Per informazioni sull'installazione di DeviceLock Enterprise Manager, leggere la sezione Installazione delle console di gestione.

Per eseguire DeviceLock Enterprise Manager, fare clic sul pulsante **Start**, scegliere **Tutti i programmi** e quindi selezionare il collegamento appropriato.



Interfaccia utente

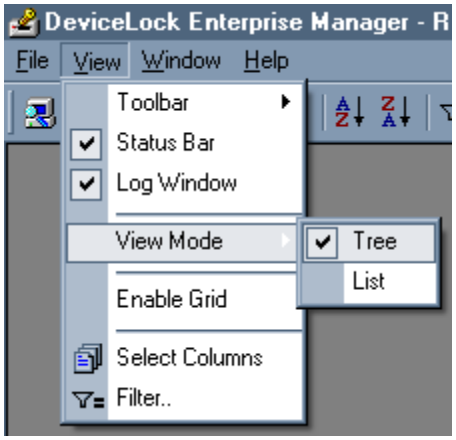
DeviceLock Enterprise Manager è dotato di un'interfaccia a documenti multipli (MDI) che consente di eseguire ciascuna operazione in una propria finestra.

La finestra principale di DeviceLock Enterprise Manager è ridimensionabile. La posizione e le dimensioni della finestra vengono automaticamente memorizzate alla chiusura della console e vengono automaticamente ripristinate all'avvio successivo del programma.

Il menu principale, visibile nella parte superiore della finestra principale, consente di accedere a tutte le principali funzioni del programma.

Per modificare la disposizione delle colonne visualizzate nelle finestre dei plug-in, selezionare **Select Columns** dal menu **View** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**.

Per impostazione predefinita, DeviceLock Enterprise Manager visualizza le informazioni ricevute dai plug-in come una struttura ad albero. Se lo si desidera, è possibile visualizzare le informazioni anche in forma di elenco. Per modificare la modalità di visualizzazione, selezionare **View Mode** dal menu **View**, quindi scegliere **Tree** oppure **List**. È necessario impostare la modalità di visualizzazione individualmente per ciascun plug-in.



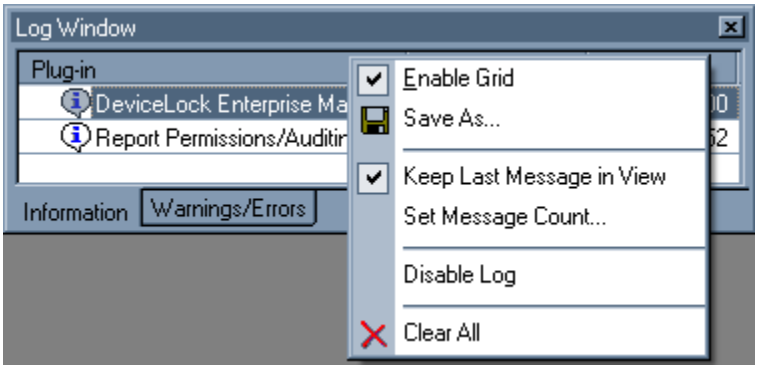
Per nascondere la barra di stato e/o la finestra delle informazioni, deselezionare le voci **Status Bar** e/o **Log Windows** dal menu **View**.

Per visualizzare la griglia nella finestra di un plug-in, selezionare **Enable Grid** nel menu **View**. La modalità scelta è indipendente per ciascun plug-in.

Per ordinare i dati visualizzati nella finestra di un plug-in, fare clic sull'intestazione della colonna che si desidera ordinare. Per invertire l'ordine di visualizzazione, fare clic una seconda volta sulla stessa intestazione di colonna.

Per visualizzare gli elementi di una struttura ad albero (quali ad esempio i nomi dei domini o dei computer) in ordine crescente o decrescente, fare clic sui relativi pulsanti sulla barra degli strumenti **Main**.

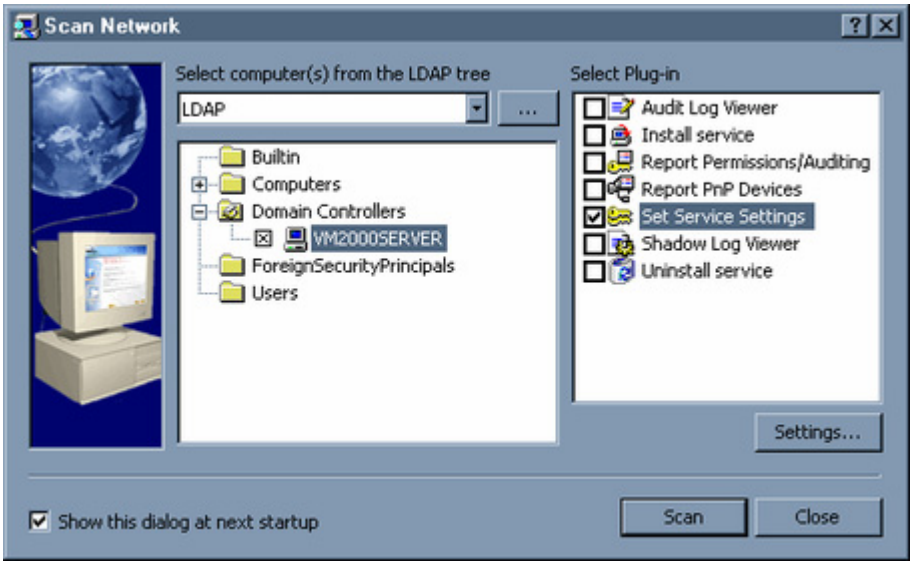
La finestra delle informazioni, visibile nella parte inferiore della finestra principale, visualizza informazioni utili sull'attività in corso ed eventuali messaggi di errore e di diagnostica. La finestra è divisa in due schede: **Information** e **Warnings/Errors**.



Per visualizzare il menu contestuale della finestra, fare clic con il pulsante destro del mouse sulla finestra stessa.

La finestra di dialogo Scan Network

La finestra di dialogo **Scan Network** consente di scegliere su quali computer connessi in rete effettuare le azioni desiderate (installazione o disinstallazione di DeviceLock Service, impostazione delle autorizzazioni e così via).



Per aprire la finestra di dialogo **Scan Network**, selezionare **Scan Network** dal menu **File** oppure fare clic sul relativo pulsante presente sulla barra degli strumenti **Main**. Se si seleziona la casella di controllo "**Show this dialog at next startup**", DeviceLock Enterprise Manager aprirà automaticamente la finestra di dialogo **Scan Network** ad ogni avvio del programma.

Per gestire DeviceLock in un ambiente di rete, sono sufficienti tre semplici passaggi.

Selezionare i computer

Il primo passaggio consiste nel selezionare i computer su cui effettuare le operazioni.

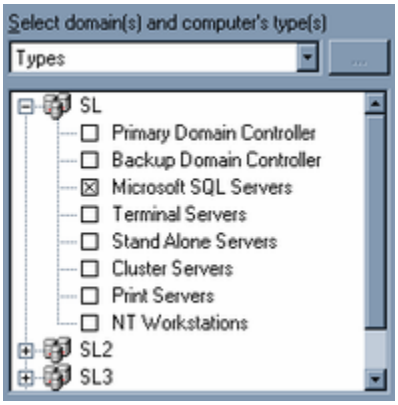
Per selezionare o deselezionare gli oggetti (tipi di computer, domini o computer), utilizzare il menu sensibile al contesto richiamabile con il pulsante destro del mouse.

DeviceLock Enterprise Manager fornisce diverse modalità per selezionare i computer connessi alla rete.

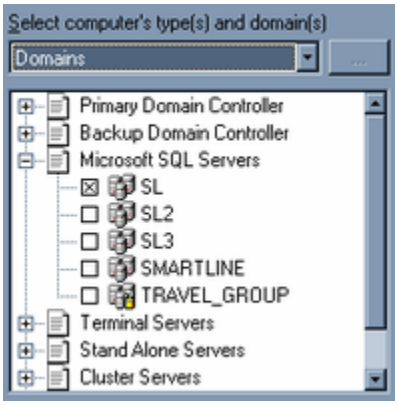
- I computer connessi in rete possono essere selezionati in base al tipo.
  Ciascun tipo rappresenta una categoria di computer:
  - **Primary Domain Controller** – controller di dominio primario.
  - **Backup Domain Controller** – backup del controller di dominio.
  - **Microsoft SQL Servers** – qualsiasi server su cui è in esecuzione Microsoft SQL Server.
  - **Terminal Servers** – qualsiasi server su cui sono attivi i servizi terminal.
  - **Stand Alone Servers** – qualsiasi server che non rappresenta un controller di dominio.
  - **Cluster Servers** – server cluster disponibile nel dominio.
  - **Print Servers** – qualsiasi computer che condivide la coda di stampa.
  - **NT Workstations** – qualsiasi workstation che esegue Windows NT, Windows 2000 o Windows XP.

  Esistono due metodi per selezionare i tipi di computer:

  1. **Types** – selezionare un dominio di rete, quindi scegliere le categorie di computer da analizzare appartenenti al dominio scelto.

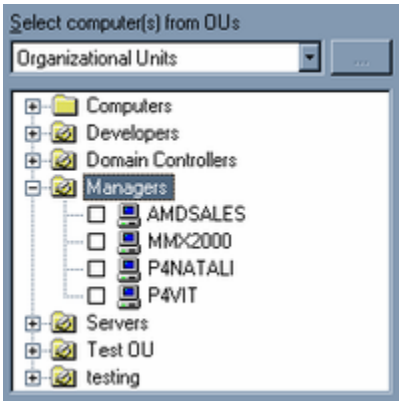
  2. **Domains** – selezionare una categoria di computer, quindi scegliere un dominio di rete all'interno del quale analizzare i computer appartenenti alla categoria scelta.



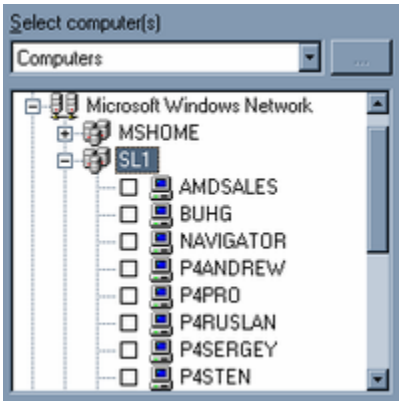
- I computer connessi in rete possono essere selezionati anche in base al proprio nome.

  È possibile scegliere un computer in base al proprio nome in diversi modi:

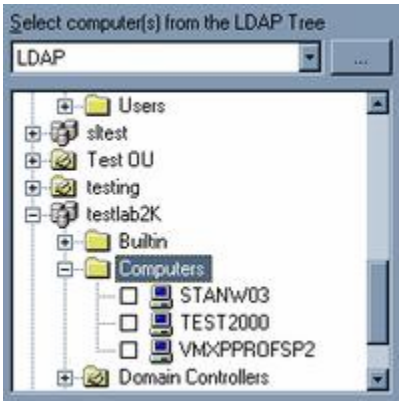
  1. **Organizational Units** – consente di esplorare le unità organizzative (OU) di Active Directory e quindi di scegliere i computer sui quali effettuare le operazioni.



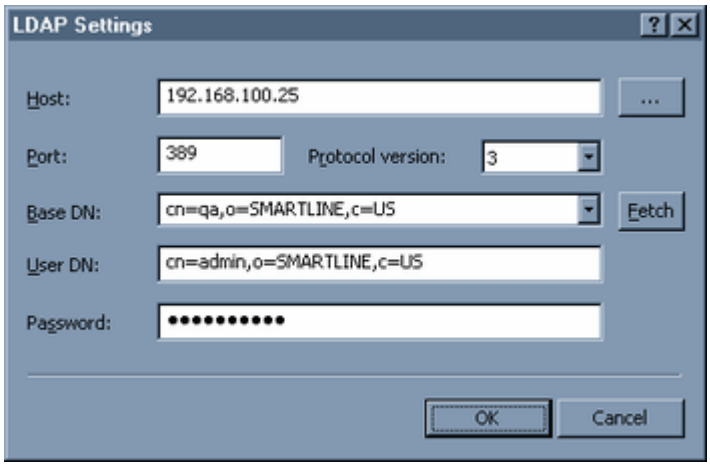
  2. **Computers** – consente di selezionare i computer dall'elenco dei computer connessi alla rete.



  3. **LDAP** – esplorare la struttura ad albero LDAP (Lightweight Directory Access Protocol) e selezionare i computer dalla directory.



Per configurare una connessione al server LDAP, fare clic sul pulsante **...**.



Host – nome o indirizzo IP del server LDAP a cui connettersi.

Port – porta TCP/IP sulla quale il server LDAP accetta le connessioni. La porta predefinita è 389.

Protocol version – versione del protocollo LDAP. Alcuni server non sono pienamente compatibili con il protocollo LDAP versione 3 e le richieste LDAP, per comunicare correttamente con tali server, devono essere corrette. Se si seleziona la **versione 2**, le richieste del server vengono corrette in base alle specifiche del protocollo LDAP versione 2.

Base DN – il punto di partenza da cui iniziare l'esplorazione della struttura della directory. È necessario utilizzare una stringa LDAP per i nomi distinti (ad esempio, cn=qa,o=SMARTLINE,c=US). Lasciare vuoto il campo **Base DN** per iniziare l'esplorazione dalla directory principale.

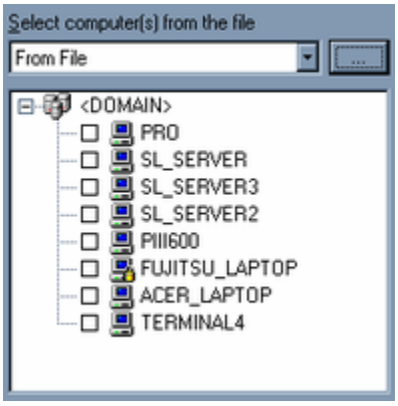
Per ottenere l'elenco di tutti i contesti dei nomi pubblicati, fare clic sul pulsante **Fetch**.

User DN – il nome distinto (DN, Distinguished name) dell'utente che consente la connessione alla directory. È necessario utilizzare una stringa LDAP per i nomi distinti (ad esempio, cn=admin,o=SMARTLINE,c=US).

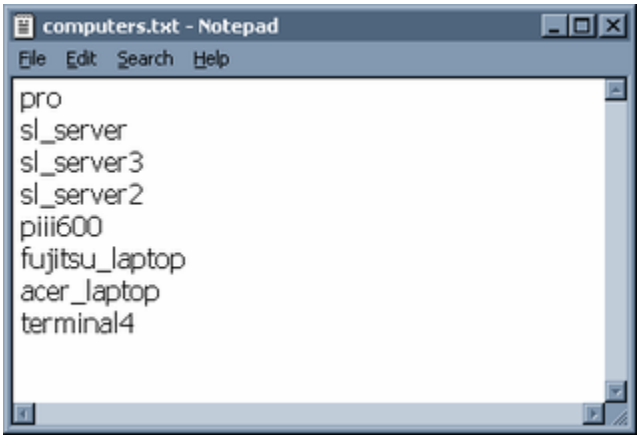
Password – password dell'utente.

4. **From File** – consente di selezionare i computer memorizzati in un file esterno predefinito.

   Per caricare un file esterno, fare clic sul pulsante **...**.

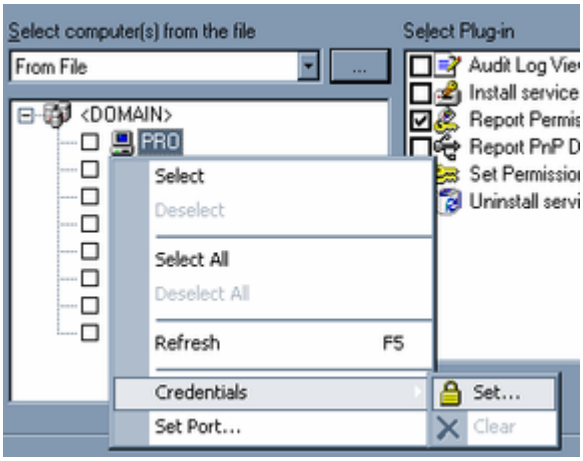


Il file esterno deve essere un documento di testo all'interno del quale è memorizzato un elenco di computer. Ogni riga del file deve rappresentare il nome di un computer o un indirizzo IP. Il file può essere sia in formato Unicode, sia in formato non Unicode. Di seguito è mostrato un esempio:



Fornire le credenziali

Se è necessario fornire credenziali alternative per connettersi ai computer della rete, evidenziare i computer o il dominio di rete elencati nella struttura ad albero, fare clic con il pulsante destro del mouse per visualizzare il menu contestuale, quindi selezionare la voce **Credentials**.

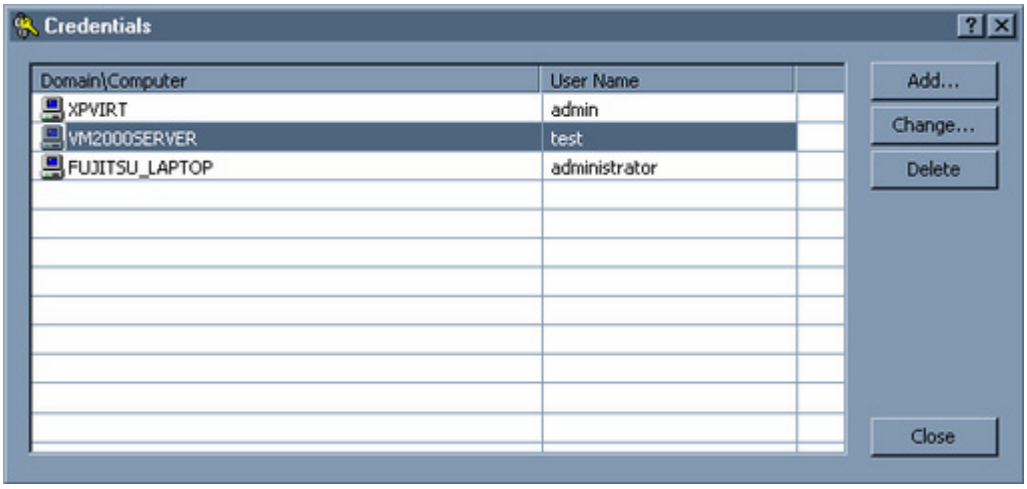


È possibile assegnare credenziali ai singoli computer e/o ai domini di rete. Per aggiungere credenziali, selezionare dal menu contestuale la voce **Set**. Per eliminare le credenziali alternative, selezionare dal menu contestuale la voce **Clear**.

Le credenziali consentono di autenticare le richieste di connessione ai computer remoti e consistono in un nome utente ed una password. Per impostazione predefinita, DeviceLock Enterprise Manager autentica le connessioni ai computer remoti ed esegue le operazioni su questi utilizzando le credenziali correnti dell'utente. Se le credenziali utilizzate dall'utente per connettersi al computer locale non dispongono dei privilegi amministrativi necessari per connettersi ai computer remoti, è necessario fornire credenziali alternative. DeviceLock Enterprise Manager utilizzerà tali credenziali alternative per autenticare automaticamente le richieste di connessione ai computer remoti.

I dati relativi alle credenziali sono memorizzati in forma crittografata e sono disponibili solo ed esclusivamente all'utente che dispone di privilegi amministrativi.

Inoltre, le credenziali possono essere fornite utilizzando la finestra di dialogo **Credentials**. Per aprire la finestra di dialogo **Credentials**, selezionare **Credentials** dal menu **File**.

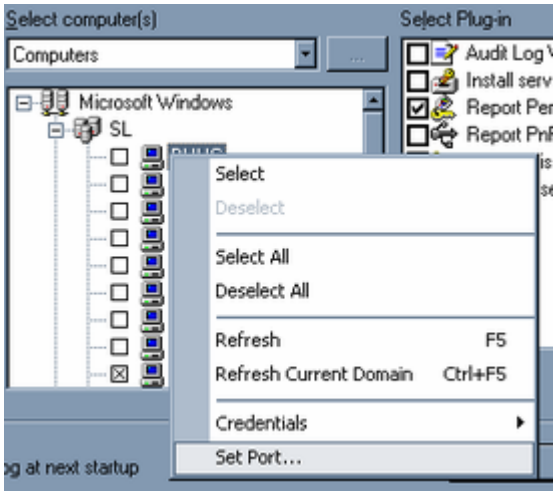


Per aggiungere nuove credenziali, fare clic sul pulsante **Add**. Per modificare le credenziali esistenti, evidenziarle e quindi fare clic sul pulsante **Change**.

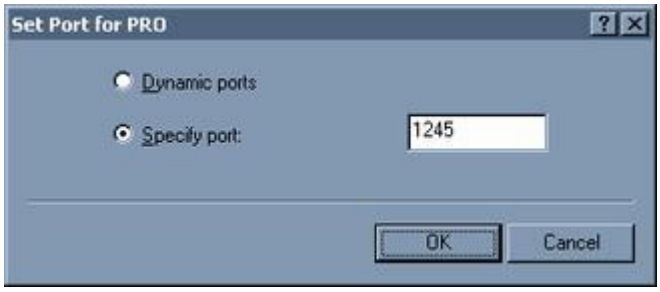
Per eliminare le credenziali, evidenziarle e quindi fare clic sul pulsante **Delete**. Per evidenziare più credenziali, utilizzare i tasti Ctrl e/o Maiusc.

Impostare una porta

Per consentire una configurazione più semplice del firewall, è possibile indicare a DeviceLock Service di utilizzare una porta fissa. A tale scopo, scegliere **Set port** dal menu contestuale.



Per impostazione predefinita, DeviceLock Enterprise Manager utilizza le porte dinamiche per la comunicazione RPC con DeviceLock Service. Comunque, è possibile indicare a DeviceLock Service di utilizzare una porta fissa. In questo caso, per consentire a DeviceLock Enterprise Manager di connettersi al computer sul quale è stato configurato DeviceLock Service, è necessario selezionare l'opzione **Specify port** e impostare il numero di porta desiderato.



Per utilizzare le porte dinamiche, selezionare l'opzione **Dynamic ports**.

Durante la fase di installazione, è possibile configurare DeviceLock Service in modo che utilizzi una porta fissa o le porte dinamiche. Per ulteriori informazioni sull'argomento, leggere le sezioni Installazione automatica e Installazione remota tramite DeviceLock Enterprise Manager.

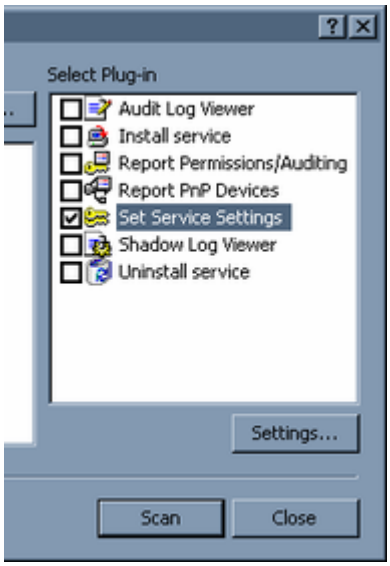
Per modificare la configurazione della porta quando DeviceLock Service è già installato, utilizzare il plug-in Install service.

Per informazioni su come configurare le porte in base alle operazioni da eseguire, leggere la sezione Plug-in.

Selezionare i plug-in

Il secondo passaggio consiste nel selezionare i plug-in che dovranno effettuare le operazioni sui computer selezionati al passaggio precedente.

Per selezionare o deselezionare un plug-in, utilizzare il menu sensibile al contesto richiamabile con il pulsante destro del mouse.



Per impostare i parametri relativi al plug-in selezionato, fare clic sul pulsante **Settings** presente nella parte inferiore dell'elenco dei plug-in. Se il plug-in selezionato non dispone di parametri addizionali, il pulsante **Settings** risulterà disattivato.

DeviceLock Enterprise Manager richiede al plug-in di eseguire le operazioni.

Il plug-in esegue la richiesta e invia le informazioni raccolte a DeviceLock Enterprise Manager. Una volta ottenute le informazioni dal plug-in, queste vengono visualizzate in una finestra separata.

Avviare una scansione

Una volta selezionati i computer e il plug-in da eseguire, è possibile avviare il processo di scansione facendo clic sul pulsante **Scan**.

Una volta avviato il processo di scansione, è possibile iniziare ad esplorare immediatamente le informazioni che sono già state raccolte dal plug-in.

Poiché la scansione di ciascun computer avviene in un thread separato, non è necessario attendere che venga completata la scansione di tutti i computer. Questo consente, inoltre, di eseguire contemporaneamente anche altre operazioni nell'interfaccia di DeviceLock Enterprise Manager.

Le uniche operazioni che non è possibile eseguire durante la scansione dei computer sono la chiusura di DeviceLock Enterprise Manager e l'esecuzione di un'altra scansione.

Se per qualsiasi motivo è necessario interrompere la scansione dei computer, selezionare **Stop Scan** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**. La scansione viene interrotta non appena un plug-in restituisce il controllo a DeviceLock Enterprise Manager.

I plug-in

DeviceLock Enterprise Manager è basato su un'architettura a plug-in flessibile che consente di utilizzare i moduli in base alle proprie esigenze. DeviceLock Enterprise Manager carica i plug-in all'avvio, dalla sottocartella ***Plugins***, memorizzata nella cartella d'installazione di DeviceLock Enterprise Manager.

DeviceLock Enterprise Manager viene fornito con una serie predefinita di plug-in che richiedono l'apertura di alcune porte sui computer remoti, come illustrato nella seguente tabella:

PORTE RICHIESTE	PLUG-IN AFFETTI
TCP 139 o TCP 445 **UDP 137** – è necessario aprire questa porta solamente quando la connessione viene stabilita in base al nome del computer. Se la connessione viene stabilita in base all'indirizzo IP, questa porta non è necessaria.	Audit Log Viewer, Report PnP Devices
TCP 139 o TCP 445 **UDP 137** – è necessario aprire questa porta solamente quando la connessione viene stabilita in base al nome del computer. Se la connessione viene stabilita in base all'indirizzo IP, questa porta non è necessaria.	Install Service, Uninstall Service

PORTE RICHIESTE	PLUG-IN AFFETTI
TCP 139 o TCP 445 **TCP 135** – questa porta è necessaria solamente quando viene utilizza la connessione con le porte dinamiche. **TCP <tutte le porte maggiori di 1024>** – queste porte sono necessarie solamente quando viene utilizza la connessione con le porte dinamiche. **TCP <porta personalizzata>** – questa porta è necessaria solamente quando viene utilizza la connessione con una porta fissa. **UDP 137** – è necessario aprire questa porta solamente quando la connessione viene stabilita in base al nome del computer. Se la connessione viene stabilita in base all'indirizzo IP, questa porta non è necessaria.	Report Permissions/Auditing, Set Service Settings, Shadow Log Viewer

Per informazioni su come configurare DeviceLock Enterprise per utilizzare una porta fissa o le porte dinamiche, leggere la sezione Impostare una porta.

Quando un plug-in è connesso ad un computer remoto, è possibile che venga visualizzato uno dei seguenti errori:

- **The product version on the client and server machines does not match (7049)** – si sta tentando la connessione a un computer su cui è installata una versione meno recente di DeviceLock Service. È necessario prima aggiornare DeviceLock Service utilizzando il plug-in Install Service.
- **The network path was not found (53)** – si sta tentando la connessione ad un computer che non esiste (il nome o l'indirizzo IP non sono validi) oppure che non è accessibile. Assicurarsi che il nome del computer specificato sia corretto. Provare ad accedere al computer tramite Windows Explorer ed effettuare la connessione utilizzando gli strumenti di amministrazione standard di Windows (quali ad esempio Gestione computer oppure Servizi).

  Questo errore si verifica inoltre quando il servizio Server di Windows non è stato avviato sul computer remoto. Verificare lo stato del servizio Server ed attivarlo se è stato arrestato.

Per la descrizione di ulteriori messaggi di errore di connessione, leggere la sezione Possibili errori di connessione.

Plug-in Audit Log Viewer

Il plug-in Audit Log Viewer consente di visualizzare il registro degli eventi di controllo di DeviceLock memorizzato nel sottosistema standard di registrazione degli eventi di Windows sul computer locale.

Per definire la dimensione massima del file registro e specificare l'operazione che Windows deve eseguire quando il registro degli eventi di controllo diventa pieno, selezionare **Audit Log Settings** dal menu contestuale.

Per cancellare il contenuto del registro, selezionare **Clear Audit** dal menu contestuale.

Per ulteriori informazioni, leggere Sezione Audit Log Viewer (Servizio).

Plug-in Install Service

Il plug-in Install Service consente di installare o aggiornare DeviceLock Service sui computer.

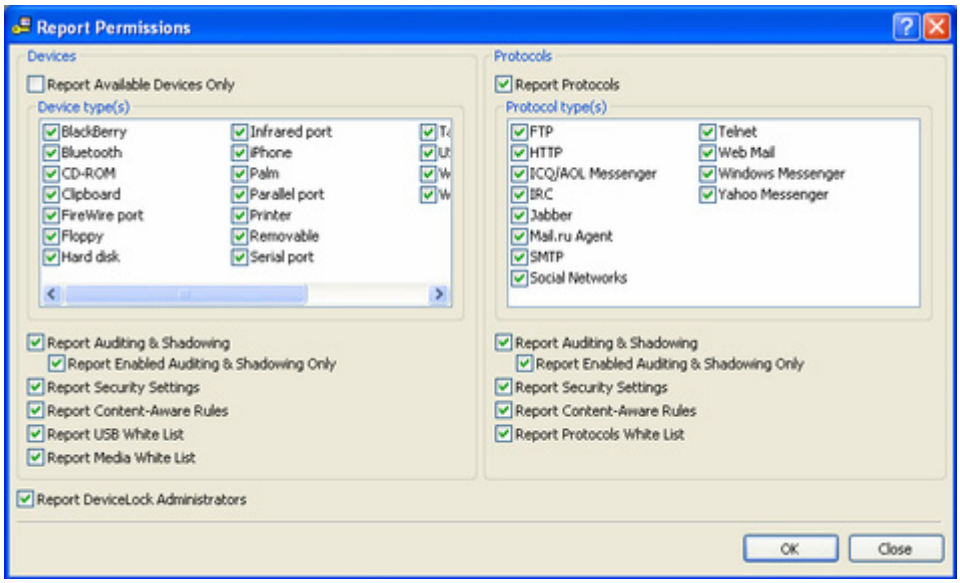
Per potere utilizzare questo plug-in, occorre selezionare la directory che contiene tutti i file necessari per l'installazione (ad esempio DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe e InstMsiW.exe). A tale scopo, fare clic sul pulsante **Settings** visibile nella parte inferiore dell'elenco dei plug-in, nella finestra di dialogo **Scan Network** (leggere la sezione Selezionare i plug-in).

Per ulteriori informazioni, leggere la sezione Installazione remota tramite DeviceLock Enterprise Manager.

Plug-in Report Permissions/Auditing

Il plug-in Report Permissions/Auditing genera un rapporto che consente di visualizzare e modificare i criteri di protezione definiti per i tipi di periferica e per i protocolli all'interno della rete.

Prima di poter utilizzare questo plug-in, è necessario selezionare le informazioni che si desiderano includere nei report. A tale scopo, fare clic sul pulsante **Settings** visibile nalla parte inferiore dell'elenco dei plug-in, nella finestra di dialogo **Scan Network** (leggere la sezione Selezionare i plug-in).



Nella finestra di dialogo **Report Permissions**, specificare le informazioni da includere nel rapporto.

Per ricevere informazioni sui criteri di protezione definiti per i tipi di periferica, utilizzare le seguenti opzioni nella sezione **Devices**:

- **Report Available Devices Only**: selezionare questa casella di controllo per generare un report in cui sono elencate le autorizzazioni e le regole di controllo impostate solamente per le periferiche correntemente disponibili sul computer. In caso contrario, sarà generato un report in cui sono elencate le autorizzazioni e le regole di controllo per tutti i tipi di periferiche supportate da DeviceLock.
- **Report Auditing & Shadowing**: selezionare questa casella di controllo per includere le regole di controllo e di shadowing. Quando questa opzione è selezionata, si ottengono informazioni anche sullo stato del **parametro Log Policy changes and Start/Stop events** (leggere la sezione Impostazioni del servizio).
- **Report Enabled Auditing & Shadowing Only**: selezionare questa casella di controllo per escludere le periferiche per cui le regole di controllo e di shadowing sono state disattivate.

  Questa opzione è disponibile solamente quando è selezionata la casella di controllo Report Auditing & Shadowing.
- **Report Security Settings**: selezionare questa casella di controllo per segnalare i parametri disattivati tramite Security Settings.
- **Report Content-Aware Rules**: selezionare questa casella di controllo per segnalare le regole basate sul contenuto impostate (consultare la sezione "Regole basate sul contenuto per le periferiche").
- **Report USB White List**: selezionare questa casella di controllo per includere le informazioni sulle periferiche incluse nella lista bianca (consultare la sezione "Lista bianca periferiche USB").
- **Report Media White List**: selezionare questa casella di controllo per includere le informazioni sulle unità incluse nella lista bianca (consultare la sezione "Lista bianca unità").
- **Report DeviceLock Administrators**: selezionare questa casella di controllo per includere gli account in grado di amministrare DeviceLock o di visualizzarne le impostazioni ed i file registro.

Per ricevere informazioni sui criteri di protezione definiti per i protocolli, utilizzare le seguenti opzioni nella sezione **Protocols**:

- **Report Protocols**: selezionare questa casella di controllo per segnalare i criteri di protezione per i protocolli. In caso contrario, le informazioni su tutti i criteri basati sui protocolli verranno escluse dal rapporto.

  Se la casella di controllo Report Protocols non è selezionata, le opzioni Report Auditing & Shadowing e Report Enabled Auditing & Shadowing Only non sono disponibili.

- **Report Auditing & Shadowing**: selezionare questa casella di controllo per segnalare le regole di controllo e shadowing impostate per i protocolli.
- **Report Enabled Auditing & Shadowing Only**: selezionare questa casella di controllo per escludere i protocolli per cui le regole di controllo e shadowing sono disattivate dal rapporto.
  Questa opzione è disponibile solo se la casella di controllo Report Auditing & Shadowing è selezionata.
- **Report Security Settings**: selezionare questa casella di controllo per segnalare i parametri definiti tramite Security Settings.
- **Report Content-Aware Rules**: selezionare questa casella di controllo per segnalare le regole basate sul contenuto impostate per i protocolli (consultare la sezione "Regole basate sul contenuto per i protocolli").
- **Report Protocols White List**: selezionare questa casella di controllo per includere le informazioni sui protocolli inclusi nella lista bianca (consultare la sezione "Gestione della lista bianca dei protocolli").

Questo report include sempre informazioni sui certificati di DeviceLock installati e sullo stato del parametro **Use Group Policy** (leggere la sezione Impostazioni del servizio).

Plug-in Report PnP Devices

Il plug-in Report PnP Devices consente di generare un report in cui sono elencate le periferiche USB, FireWire e PCMCIA correntemente e precedentemente collegate al computer.

Nota: per recuperare le periferiche PnP dai computer con sistema operativo Windows Vista/7 e Windows Server 2008, occorre autorizzare l'accesso remoto all'interfaccia PnP su tali computer. Per farlo, modificare i criteri seguendo le istruzioni del seguente articolo: http://support.microsoft.com/kb/947040/it.

Di seguito sono descritte le colonne visualizzate nel report:

- **Description** – mostra la descrizione della periferica fornita dal produttore.
- **Device Information** – mostra informazioni addizionali relative alla periferica fornite dal produttore.
- **Connected to** – mostra il tipo di interfaccia a cui è collegata la periferica (USB, FireWire o PCMCIA).
- **Class** – mostra la classe di appartenenza della periferica riportata dal sistema operativo.
- **Class description** – mostra la descrizione della periferica riportata dal sistema operativo.
- **Present** – indica se la periferica è correntemente connessa o meno (valori possibili:**Yes** o **No**).

- **DeviceID** – mostra la stringa di identificazione univoca della periferica fornita dal produttore.
- **Driver** – mostra il nome del driver che controlla la periferica.

Per aggiungere le periferiche USB al database delle periferiche USB, utilizzare il menu contestuale richiamabile facendo clic con il pulsante destro del mouse.

Prima di poter utilizzare questo plug-in, è necessario selezionare le informazioni che si desiderano includere nei report. A tale scopo, fare clic sul pulsante **Settings** visibile nalla parte inferiore dell'elenco dei plug-in, nella finestra di dialogo **Scan Network** (leggere la sezione Selezionare i plug-in).

- **Report Connected Devices Only** – selezionare questa casella di controllo per generare un report in cui sono elencate le periferiche correntemente collegate al computer. In caso contrario, sarà generato un report in cui sono elencate anche le periferiche che erano state precedentemente collegate al computer.
- **Report FireWire Devices** – selezionare questa casella di controllo per includere le periferiche che sono collegate alla porta FireWire.
- **Report PCMCIA Devices** – selezionare questa casella di controllo per includere le periferiche che sono collegate allo slot PCMCIA.
- **Report USB Devices** – selezionare questa casella di controllo per includere le periferiche che sono collegate alla porta USB.

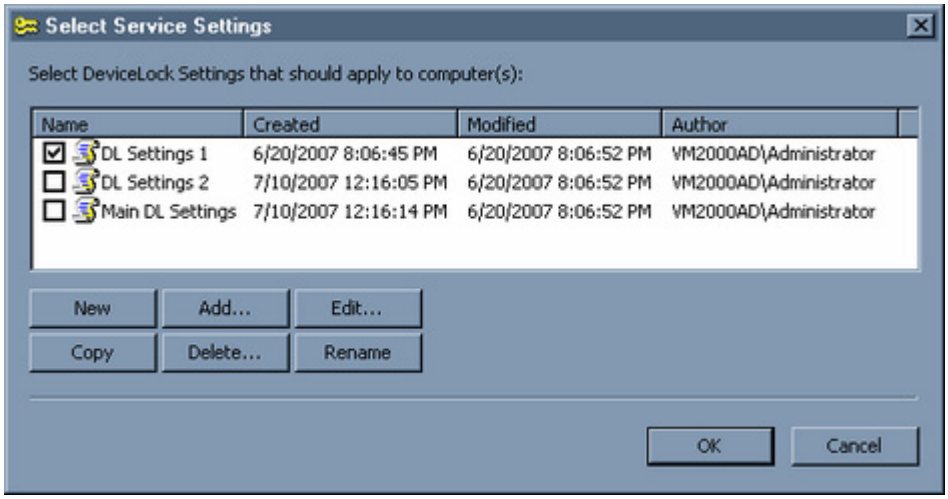
Plug-in Set Service Settings

Il plug-in Set Service Settings legge il criterio (impostazioni, autorizzazioni, regole di controllo e di shadowing) dal file XML esterno e lo distribuisce agli agenti DeviceLock Service dell'intera rete.

Nota: solo le impostazioni espressamente definite in un file di criteri vengono applicate ai computer client. Tutte le impostazioni di criteri con lo stato **Not Configured** vengono ignorate dai computer client.

Prima di poter utilizzare questo plug-in, è necessario definire le impostazioni, le autorizzazioni e/o le regole di controllo che si desiderano distribuire. A tale scopo, fare clic

sul pulsante **Settings** visibile nalla parte inferiore dell'elenco dei plug-in, nella finestra di dialogo **Scan Network** (leggere la sezione Selezionare i plug-in).



È innanzitutto necessario preparare il criterio da distribuire.

Se l'elenco non include alcun file, è possibile creare un file vuoto facendo clic sul pulsante **New** o aggiungere un file esistente facendo clic sul pulsante **Add**.

Selezionare quindi il file nell'elenco e fare clic sul pulsante **Edit** per avviare DeviceLock Service Settings Editor. DeviceLock Service Settings Editor è utilizzato per creare e modificare file XML esterni introducendo impostazioni, autorizzazioni, regole di controllo e di shadowing per DeviceLock Service. Per ulteriori informazioni, consultare la sezione DeviceLock Service Settings Editor di questo manuale.

Una volta modificato il criterio, selezionare il file corrispondente spuntando la casella di controllo posta accanto al nome del file nell'elenco. Quindi fare clic sul pulsante **OK** per chiudere la finestra di dialogo di configurazione.

Plug-in Shadow Log Viewer

Il plug-in Shadow Log Viewer consente di visualizzare il registro di shadowing di DeviceLock Service.

Per accedere a tutte le funzioni di questo plug-in, utilizzare il menu sensibile al contesto richiamabile con il pulsante destro del mouse.

Per ulteriori informazioni sull'argomento, leggere Sezione Shadow Log Viewer (Servizio).

Plug-in Uninstall Service

Il plug-in Uninstall Service consente di disinstallare DeviceLock Service e tutti i relativi componenti dai computer.

Se l'utente connesso al computer non dispone di accesso amministrativo a DeviceLock Service, il plug-in non sarà in grado di rimuovere il servizio.

Inoltre, se l'utente non dispone di privilegi amministrativi locali sul computer su cui è in esecuzione DeviceLock Service, si verificherà un errore.

Aprire, salvare, esportare i dati raccolti

DeviceLock Enterprise Manager consente di salvare tutte le informazioni ricevute dai plug-in.

I dati possono essere memorizzati in un file esterno, richiamabile da DeviceLock Enterprise Manager quando necessario.

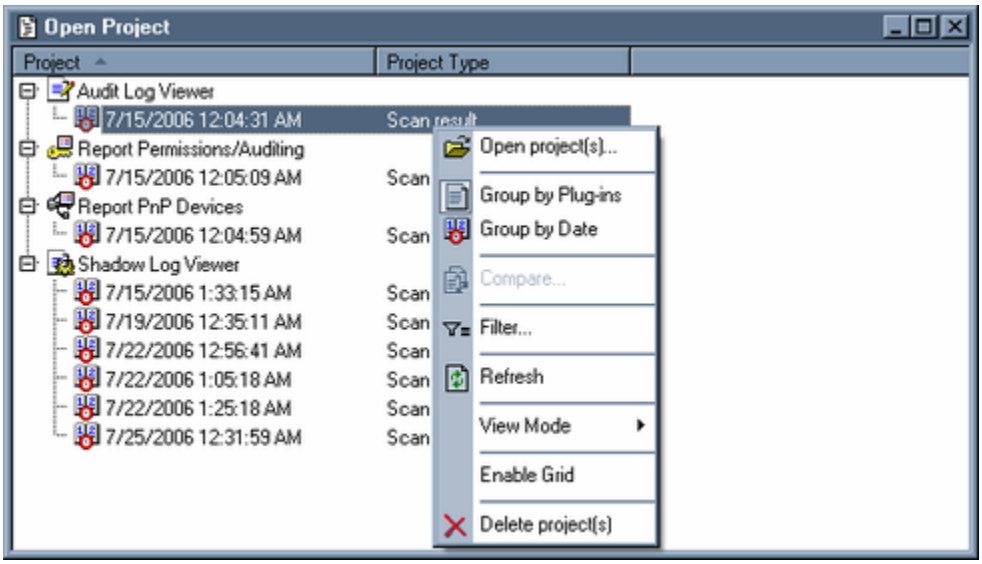
Sono disponibili tre metodi per salvare e caricare i dati:

1. Il metodo più semplice per salvare le informazioni consiste nel memorizzarle in un file progetto. Quando si salvano i dati in un file progetto, DeviceLock Enterprise Manager memorizza il contenuto della finestra di ciascun plug-in attivo in un file separato e lo salva nella sottocartella ***Project***.

   I nomi dei file progetto sono assegnati automaticamente, in base al nome del plug-in e in base alla data e all'ora in cui è stata avviata la scansione.

   Per salvare i dati in un file progetto, selezionare **Save Project** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**.

   Per aprire un file progetto precedentemente salvato, selezionare **Open Project** dal menu **File**.



   La finestra di dialogo **Open Project** dispone di una propria barra degli strumenti e di un proprio menu contestuale.

   È possibile raggruppare i file progetto precedentemente salvati in base alla data di scansione e in base al tipo di informazioni memorizzate. Selezionare **Group by Type**

o **Group by Date** dal menu contestuale oppure fare clic sui relativi pulsanti sulla barra degli strumenti **Project**.

Per aprire un file progetto, selezionarlo dall'elenco dei file progetto, quindi fare clic sul pulsante **Open Project** sulla barra degli strumenti **Project**. Per selezionare più file progetto contemporaneamente, utilizzare i tasti Ctrl e/o Maiuscolo.

2. Un altro metodo per salvare le informazioni recuperate dai plug-in consiste nel selezionare **Save As** dal menu **File**. Questo consente di salvare i dati in un file di tipo ANM e di memorizzarlo su disco fisso o su qualsiasi altro supporto con un nome di propria scelta.

   Per aprire un file precedentemente salvato, selezionare **Open** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**. È necessario specificare il nome del file che si desidera aprire. È possibile aprire solamente i file di tipo ANM.

3. Per consentire ad un'applicazione esterna di importare le informazioni raccolte da DeviceLock Enterprise Manager, è necessario esportare i dati in un file esterno. Per esportare i dati, selezionare **Save As** dal menu **File**, quindi scegliere dalla casella combinata Tipo file il tipo di file da creare. DeviceLock Enterprise Manager consente la creazione di file in formato MS Excel (se l'applicazione è installata sul computer locale) e di file di testo delimitati da tabulazioni (TXT) e delimitati da virgole (CSV).

   Se si esportano i dati in un file esterno, questo non sarà più importabile in DeviceLock Enterprise Manager poiché DeviceLock Enterprise Manager è in grado di aprire solamente i file nel formato proprietario ANM. Esportare i dati in un file esterno è utile qualora si desideri scambiare le informazioni tra DeviceLock Enterprise Manager e altre applicazioni.

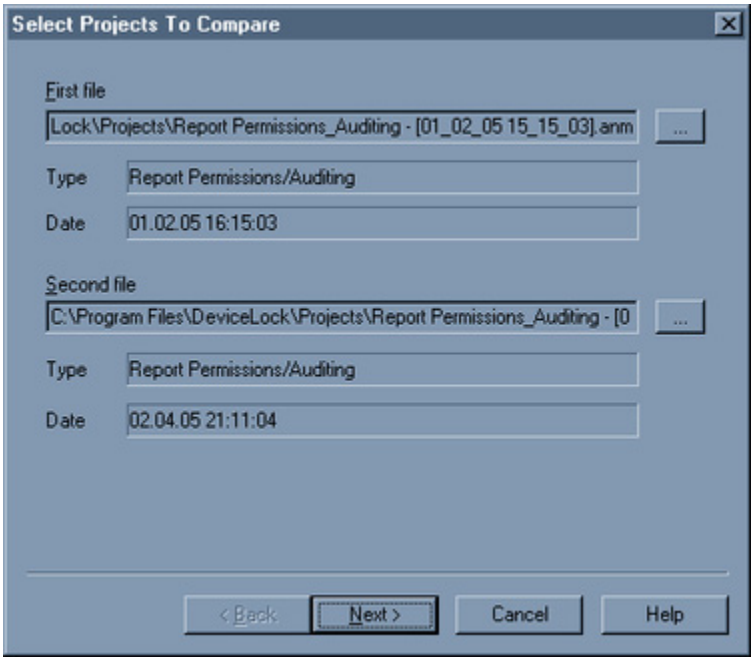
Confrontare i dati

DeviceLock Enterprise Manager consente di tenere traccia delle modifiche apportate ai computer collegati alla rete confrontando tra loro due file progetto salvati in precedenza. Questo si rivela particolarmente utile quando il numero di computer da amministrare è particolarmente alto.

DeviceLock Enterprise Manager fornisce una procedura guidata utile e intuitiva che consente di confrontare tra loro due file ANM. Per eseguire la procedura guidata, selezionare **Compare** dal menu **File**.

Per confrontare il contenuto di due file ANM, è sufficiente eseguire tre passaggi, come illustrato di seguito.

1. Innanzitutto, è necessario selezionare i file che si desiderano confrontare.

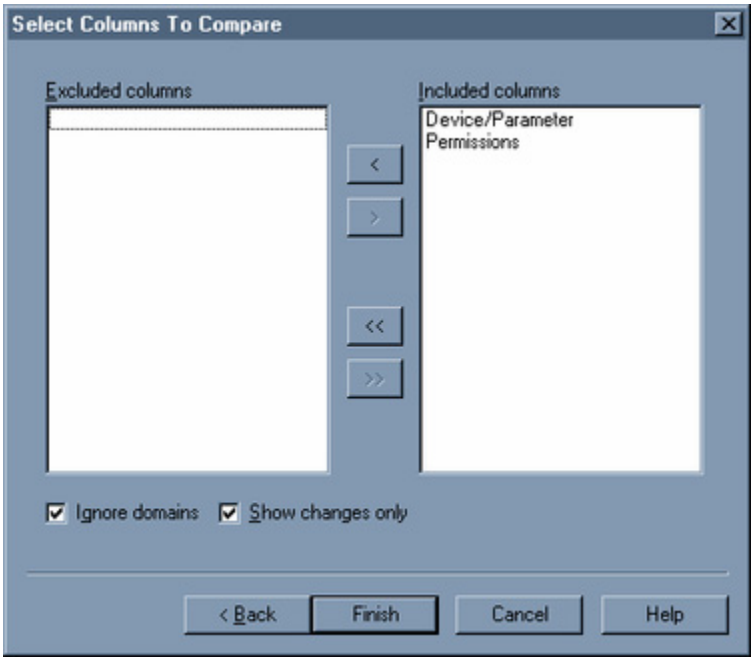


Per scegliere il primo e il secondo file da confrontare, fare clic sui relativi pulsanti **...**.

Nota: è possibile confrontare tra loro solo file dello stesso tipo. Non è possibile, ad esempio, confrontare le informazioni raccolte dal plug-in Report Permissions/Auditing con le informazioni raccolte dal plug-in Report PnP Devices.

Una volta selezionati i due file da confrontare, scegliere **Avanti** per visualizzare la pagina successiva della procedura guidata.

2. Ora, selezionare le colonne da includere nella fase di confronto.



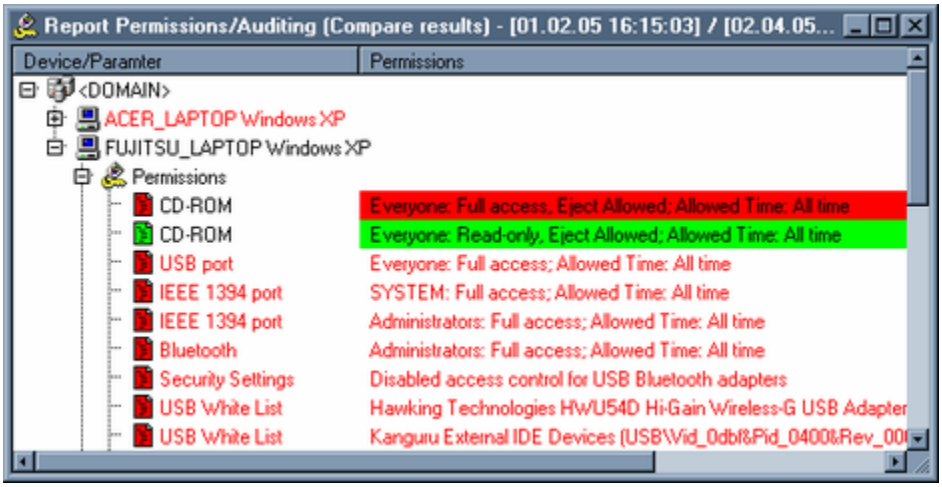
DeviceLock Enterprise Manager confronterà tra loro solo le colonne selezionate. Per escludere una colonna dalla fase di confronto, spostarla dall'elenco **Included columns** all'elenco **Excluded columns**. Le colonne escluse rimarranno comunque visibili ma i relativi contenuti saranno ignorati e non influiranno sul risultato del confronto.

Per impostazione predefinita, come risultato del confronto DeviceLock Enterprise Manager visualizzerà solo i valori che differiscono nei due file confrontati. Per visualizzare tutti i valori, inclusi quelli non modificati, deselezionare la casella di controllo **Show changes only**.

Per includere nel risultato del confronto anche i nomi dei domini di rete, deselezionare la casella di controllo **Ignore domains**. Se la casella di controllo **Ignore domains** è selezionata, DeviceLock Enterprise Manager ignorerà i domini e si limiterà a confronterà tra loro i computer e le relative informazioni.

3. Come ultimo passaggio, confrontare i file. Fare clic sul pulsante **Fine** per avviare il confronto tra i due file scelti.

   DeviceLock Enterprise Manager visualizza il risultato del confronto in una finestra separata, sotto forma di struttura ad albero, esattamente come quando visualizza le informazioni ricevute da un plug-in.


Report Permissions/Auditing (Compare results) - [01.02.05 16:15:03] / [02.04.05...
Device/Paramter
Permissions
<DOMAIN>
ACER_LAPTOP Windows XP
FUJITSU_LAPTOP Windows XP
Permissions
CD-ROM
Everyone: Full access, Eject Allowed; Allowed Time: All time
CD-ROM
Everyone: Read-only, Eject Allowed; Allowed Time: All time
USB port
Everyone: Full access; Allowed Time: All time
IEEE 1394 port
SYSTEM: Full access; Allowed Time: All time
IEEE 1394 port
Administrators: Full access; Allowed Time: All time
Bluetooth
Administrators: Full access; Allowed Time: All time
Security Settings
Disabled access control for USB Bluetooth adapters
USB White List
Hawking Technologies HWU54D Hi-Gain Wireless-G USB Adapter
USB White List
Kanguru External IDE Devices (USB\Vid_0dbf&Pid_0400&Rev_00

L'algoritmo utilizzato per il confronto delle informazioni è semplice ed efficace:

1. Se la casella di controllo **Ignore domains** è deselezionata, il programma enumera i domini di rete presenti nei due file selezionati, quindi cerca ciascun dominio di rete sia nel primo file, sia nel secondo file.

   Se il dominio di rete esiste nel file più vecchio ma non esiste nel file più recente, DeviceLock Enterprise Manager include il dominio di rete mancante (inclusi i computer appartenenti a tale dominio e le informazioni raccolte) nel risultato del confronto ed evidenzia in rosso i dati differenti.

   Se il dominio di rete non esiste nel file più vecchio ma esiste nel file più recente, DeviceLock Enterprise Manager include il dominio di rete mancante (inclusi i computer appartenenti a tale dominio e le informazioni raccolte) nel risultato del confronto ed evidenzia in verde i dati differenti.

Se il dominio di rete esiste in entrambi i file, DeviceLock Enterprise Manager enumera tutti i computer appartenenti a quel dominio (vedere sotto).

2. Se la casella di controllo **Ignore domains** è selezionata, DeviceLock Enterprise Manager ignora i domini di rete ed enumera tutti i computer presenti nei due file selezionati, quindi cerca ciascun computer sia nel primo file che nel secondo file.

   Se il computer esiste nel file più vecchio ma non esiste nel file più recente, DeviceLock Enterprise Manager include il computer mancante e le relative informazioni nel risultato del confronto ed evidenzia in rosso i dati differenti.

   Se il computer non esiste nel file più vecchio ma esiste nel file più recente, DeviceLock Enterprise Manager include il computer mancante e le relative informazioni nel risultato del confronto ed evidenzia in verde i dati differenti.

   Se il computer esiste in entrambi i file, DeviceLock Enterprise Manager enumera tutte le informazioni raccolte (vedere sotto).

3. DeviceLock Enterprise Manager enumera tutte le informazioni relative ad un computer, quindi cerca ciascun dato sia nel primo file sia nel secondo file.

   Se il dato è presente nel file più vecchio ma non è presente nel file più recente, DeviceLock Enterprise Manager visualizza il dato mancante nel risultato del confronto e lo evidenzia in rosso.

   Se il dato non esiste nel file più vecchio ma esiste nel file più recente, DeviceLock Enterprise Manager visualizza il dato mancante nel risultato del confronto e lo evidenzia in verde.

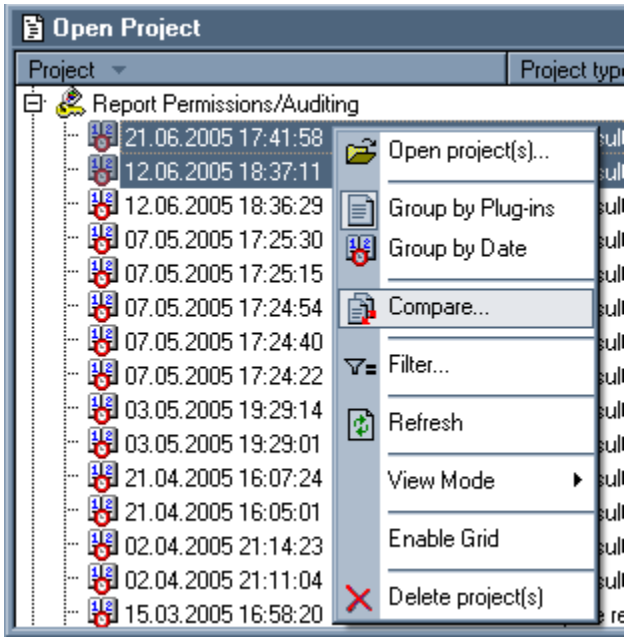
   Se il dato è presente in entrambi i file, DeviceLock Enterprise Manager avvia il confronto del contenuto di ciascuna colonna:

   - Se i valori della colonna relativa al primo file sono differenti dai valori della colonna relativa al secondo file, DeviceLock Enterprise Manager include entrambi i valori nel risultato del confronto. Il valore appartenente al file più recente viene visualizzato subito dopo il valore appartenente al file più vecchio.

     La colonna che contiene il valore più vecchio è evidenziata in rosso. La colonna che contiene il valore più recente è evidenziata in verde Le colonne escluse dal confronto o che presentano valori uguali non sono evidenziate ma sono mostrate nel colore predefinito.

   - Se tutti i valori della colonna appartenente al file più vecchio sono uguali ai valori della colonna appartenente al file più recente, DeviceLock Enterprise Manager ignora tali valori (se la casella di controllo **Show changes only** è selezionata) oppure include il valore nel risultato del confronto e lo visualizza nel colore predefinito (se la casella di controllo **Show changes only** è deselezionata).

Se si desidera confrontare tra loro due file progetto, si consiglia di utilizzare la funzione speciale disponibile nella finestra di dialogo **Open Project**.



Selezionare **Open Project** dal menu **File**, evidenziare i due file progetto da confrontare (è possibile utilizzare i tasti Ctrl e/o Maiuscolo per selezionare contemporaneamente i due file progetto), quindi scegliere **Compare** dal menu contestuale oppure fare clic sul relativo pulsante sulla barra degli strumenti **Project**.

Nota: è possibile selezionare solamente due file progetto ed entrambi devono essere dello stesso tipo.

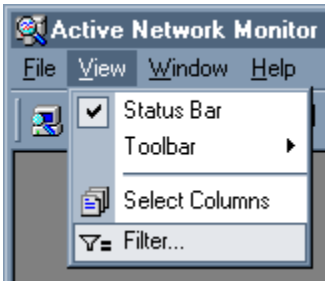
DeviceLock Enterprise Manager mette a disposizione due pulsanti sulla barra degli strumenti **Compare** che consentono di esplorare il risultato del confronto. Il pulsante **<** consente di evidenziare il dato precedente che presenta modifiche. Il pulsante **>** consente di evidenziare il dato successivo che presenta modifiche.

È possibile salvare il risultato del confronto in un file ANM o esportarlo in documento MS Excel oppure in un documento di testo (file con estensione TXT o CSV). Per salvare o esportare il risultato del confronto, selezionare **Save As** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**.

Così come ogni altro file di DeviceLock Enterprise Manager, un volta salvato il risultato del confronto in un file, questo può essere aperto in DeviceLock Enterprise Manager. Per aprire un file in cui è memorizzato il risultato di un confronto, scegliere **Open** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**, quindi specificare il nome del file da aprire. È possibile aprire solo file in formato ANM.

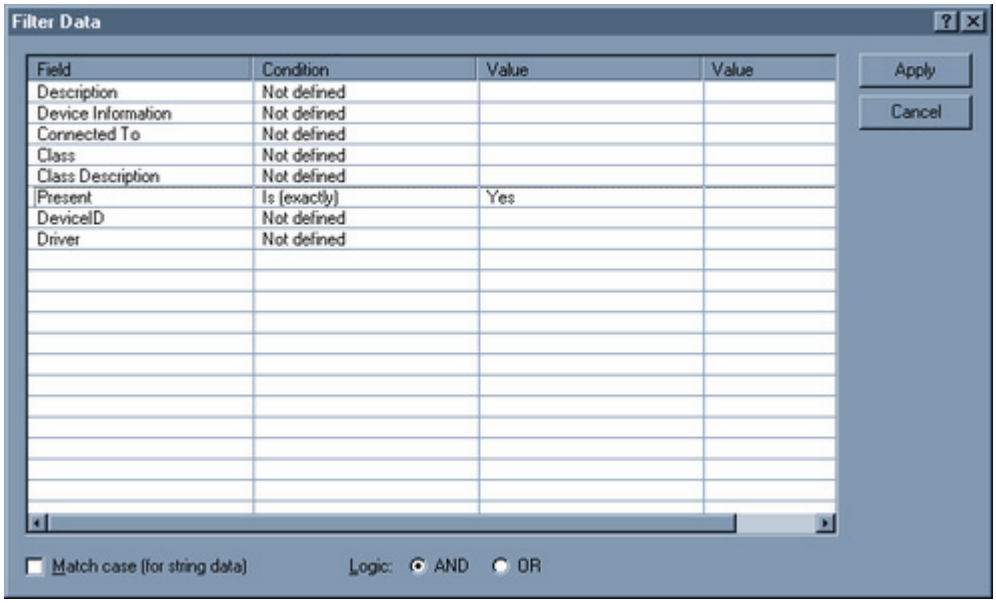
Filtrare i dati

DeviceLock Enterprise Manager è dotato di una funzione sofisticata in grado di filtrare i dati e che consente di visualizzare solo le informazioni desiderate in base ai criteri specificati.



Per aprire la finestra di dialogo **Filter Data**, scegliere **Filter** dal menu **View** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**.

Nota: per poter filtrare i dati, è necessario che sia visibile la finestra con i risultati della scansione della rete o del confronto tra due file.



- La colonna **Field** contiene tutti i campi relativi al risultato del confronto o della scansione che è possibile filtrare. È possibile definire un operatore logico **AND** oppure **OR** per ciascun campo individualmente:

  AND - operatore logico che include solo i record che soddisfano tutte le condizioni richieste. Ad esempio, il filtro Process = "explorer.exe" AND PID = 3764 visualizza tutti i dati che soddisfano sia la condizione Process = "explorer.exe", sia la condizione PID = 3764. Il filtro non visualizza i dati che soddisfano la condizione Process = "explorer.exe" ma non soddisfano la condizione PID = 3764 o viceversa.

  OR – operatore logico che include tutti i record che soddisfano almeno una delle condizioni richieste. Ad esempio, il filtro Process = "explorer.exe" OR PID = 3764 visualizza tutti i dati che soddisfano una od entrambe le condizioni, ovvero quando Process = "explorer.exe" (indipendentemente che la condizione PID = 3764 sia soddisfatta o meno) o quando PID = 3764 (indipendentemente che la condizione Process = "explorer.exe" sia soddisfatta o meno).

- La colonna **Condition** contiene un elenco di operazioni logiche che è possibile eseguire sul campo selezionato. È possibile selezionare solo un'operazione logica per ciascun campo. DeviceLock Enterprise Manager supporta due gruppi di operazioni logiche, una per i dati di tipo stringa e una per i dati di tipo non stringa.

  Di seguito sono elencate le operazioni logiche che è possibile eseguire sui dati di tipo stringa (la stringa di destinazione rappresenta la stringa di testo utilizzata come argomento dall'operazione logica, ad esempio "explorer.exe"):

  - **Is (exactly)** – seleziona solo i dati le cui stringhe di testo sono identiche alla stringa di destinazione.

- **Includes** – seleziona solo i dati le cui stringhe di testo includono la stringa di destinazione.
- **Is not** – seleziona solo i dati le cui stringhe di testo sono differenti dalla stringa di destinazione.
- **Not includes** – seleziona solo i dati le cui stringhe di testo non includono la stringa di destinazione.
- **Empty** – seleziona solo i dati i cui campi sono vuoti.
- **Not Empty** – seleziona solo i dati i cui campi non sono vuoti.
- **Regular expression** – seleziona solo i dati le cui stringhe di testo corrispondono ad una espressione. L'espressione può contenere i caratteri jolly, ad esempio "explorer*".

Se si desidera che il confronto tra stringhe di testo tenga conto della differenza tra caratteri maiuscoli e minuscoli (ad esempio, si desidera che la stringa "Explorer.exe" sia considerata differente dalla stringa "explorer.exe"), selezionare la casella di controllo **Match case**. Se la casella di controllo **Match case** è deselezionata, il confronto tra stringhe di testo non terrà conto della differenza tra caratteri maiuscoli e minuscoli (riprendendo l'esempio precedente, la stringa "Explorer.exe" è considerata identica alla stringa "explorer.exe").

Le operazioni logiche che è possibile eseguire sui dati di tipo non stringa sono:

Se non si desidera eseguire un'operazione logica su un campo, selezionare **Not defined** dall'elenco delle operazioni logiche.

- Le colonne **Value** contengono gli argomenti definiti dall'utente. La seconda colonna **Value** diventa disponibile solamente quando viene selezionata l'operazione logica **Between (in)** o **Not Between (out)**. Per tutte le altre operazioni logiche, è necessaria solamente la prima colonna **Value**.

Una volta definiti i criteri di filtraggio, fare clic sul pulsante **Apply** per applicare i filtri ai dati.

È possibile salvare il risultato dell'operazione di filtraggio in un file ANM o esportarlo in documento MS Excel oppure in un documento di testo (file con estensione TXT o CSV). Per salvare o esportare il risultato dell'operazione di filtraggio, selezionare **Save As** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**.

Così come ogni altro file di DeviceLock Enterprise Manager, un volta salvato il risultato dell'operazione di filtraggio in un file, questo può essere aperto in DeviceLock Enterprise Manager. Per aprire un file, scegliere **Open** dal menu **File** oppure fare clic sul relativo pulsante sulla barra degli strumenti **Main**, quindi specificare il nome del file da aprire. È possibile aprire solo i file che sono stati precedentemente salvati da DeviceLock Enterprise Manager.

Regole basate sul contenuto per le periferiche (Regular Profile)

Le regole basate sul contenuto (Content-Aware Rules) migliorano la funzionalità di base del controllo dell'accesso alle porte/periferiche di DeviceLock, aggiungendo una protezione completa a livello di file dei documenti aziendali contenenti informazioni riservate. Le regole basate sul contenuto consentono di eseguire l'ispezione automatica del contenuto dei dati copiati sulle periferiche di memorizzazione esterne, il rilevamento del contenuto riservato e l'applicazione dei criteri normativi allo scopo di garantire la protezione.

Le regole basate sul contenuto consentono di concedere o negare in maniera selettiva l'accesso a determinati contenuti dei file, indipendentemente dalle autorizzazioni prestabilite a livello di tipo di periferica. Le regole basate sul contenuto, inoltre, possono essere utilizzate per autorizzare o negare la copia shadow di determinati contenuti. Le regole basate sul contenuto sono flessibili e possono essere definite a livello di utente o di gruppo.

È possibile configurare le regole basate sul contenuto per le operazioni di controllo dell'accesso, per le operazioni di copia shadow, o per entrambe.

Seguono alcuni esempi di utilizzo delle regole basate sul contenuto (Content-Aware Rules).

- **Esempio 1 - Utilizzo delle regole basate sul contenuto per le operazioni di controllo dell'accesso**. È possibile autorizzare determinare utenti o gruppi a leggere i file contenenti la frase “Distribuzione vietata” dalle periferiche Removable, Floppy e CD/DVD e, allo stesso tempo, impedire loro di scrivere sui file contenenti più di un numero di carta di credito sulle periferiche Removable e Floppy.
- **Esempio 2 - Utilizzo delle regole basate sul contenuto per le operazioni di copia shadow**. È possibile specificare l'esecuzione della copia shadow solo per i file contenenti numeri di carta di credito, codici fiscale, le parola “Segreto”, “Riservato”, “Limitato” e le frasi “Top Secret” e “Solo per uso ufficiale”, ai fini delle verifiche di sicurezza e delle indagini sugli incidenti.

Nota: è possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Le regole basate sul contenuto online (Regular Profile) si applicano ai computer client che operano online. Le regole basate sul contenuto offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione “Criteri di protezione DeviceLock (Offline Profile)”. Per informazioni su come definire le regole basate sul contenuto offline, consultare la sezione “Gestione delle regole basate sul contenuto offline per le periferiche”.

Regole basate sul contenuto per le operazioni di controllo dell'accesso

Quando le regole basate sul contenuto vengono applicate alle operazioni di controllo dell'accesso, gestiscono le operazioni di lettura, scrittura ed eliminazione dei contenuti specificati. Le operazioni di eliminazione e scrittura vengono controllate insieme.

Le regole basate sul contenuto consentono di:

- Autorizzare l'accesso in lettura/scrittura a determinati contenuti dei file quando l'accesso è negato a livello di tipo di periferica.
- Negare l'accesso in lettura/scrittura a determinati contenuti dei file quando l'accesso è autorizzato a livello di tipo di periferica.

Nota: DeviceLock può controllare l'accesso alle periferiche a due livelli: interfaccia (porta) e tipo. Per alcune periferiche il controllo viene eseguito per entrambi i livelli, per altre per un solo livello, interfaccia (porta) o tipo. Ad esempio, un'unità flash USB rientra in entrambi i livelli: interfaccia (USB) e tipo (Removable). Le regole basate sul contenuto funzionano solo se il controllo dell'accesso avviene a livello di tipo (Removable, Floppy, ecc.) DeviceLock non esegue il controllo dell'accesso per le periferiche USB a livello di tipo se si verificano le seguenti condizioni:

- La periferica non viene aggiunta all'elenco USB Devices White List, **Access control for USB storage devices** è abilitato in Security Settings e l'utente non ha accesso al tipo di periferica porta **USB**.

OPPURE

- La periferica viene aggiunta all'elenco USB Devices White List e la casella di controllo **Control As Type** non è selezionata.

La seguente tabella fornisce un riepilogo dei diritti di accesso che possono essere specificati nelle regole basate sul contenuto.

DIRITTI DI ACCESSO	DESCRIZIONE
Generic: Read	Determina se l'utente può leggere determinati contenuti da una periferica. Si applica ai tipi di periferica DVD/CD–ROM, Floppy e Removable.
Generic: Write	Determina se l'utente può scrivere determinati contenuti su una periferica. Si applica ai tipi di periferica Floppy e Removable.
Generic: Read, Write	Determina se l'utente può leggere e scrivere determinati contenuti da e su una periferica. Si applica ai tipi di periferica Floppy e Removable.
Encrypted: Read	Determina se l'utente può leggere determinati contenuti da una periferica crittografata. Si applica unicamente al tipo di periferica Removable.
Encrypted: Write	Determina se l'utente può scrivere determinati contenuti su una periferica crittografata. Si applica unicamente al tipo di periferica Removable.
Encrypted: Read, Write	Determina se l'utente può leggere e scrivere determinati contenuti da e su una periferica crittografata. Si applica unicamente al tipo di periferica Removable.

Nota: i diritti di accesso generico specificati per il tipo di periferica Removable si applicano solo alle periferiche non crittografate. I diritti di accesso crittografato specificati per il tipo di periferica Removable si applicano solo alle periferiche crittografate. Per specificare i diritti di accesso per entrambi i tipi di periferica Removable (crittografati e non crittografati), occorre specificare entrambi i diritti di accesso, generico e crittografato. Per informazioni dettagliate sulle periferiche riconosciute da DeviceLock Service come crittografate, consultare la sezione "Crittografia".

La seguente tabella mostra come le diverse autorizzazioni a livello di tipo periferica e a livello di file influenzano lo stato di un'autorizzazione per un account utente. Le autorizzazioni a livello di tipo periferica vengono impostate per un tipo di periferica. Le autorizzazioni a livello di file vengono definite dalle regole basate sul contenuto.

	FULL ACCESS livello tipo periferica	**NO ACCESS** livello tipo periferica	**ALLOW READ/ DENY WRITE** livello tipo periferica
ALLOW READ livello file	autorizza l'accesso in lettura a tutti i contenuti, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in lettura a tutti i contenuti, tranne a quelli specificati, nega la creazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	autorizza l'accesso in lettura a tutti i contenuti, nega la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
DENY READ livello file	nega l'accesso in lettura ai contenuti specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso a una periferica	nega l'accesso in lettura ai contenuti specificati, nega la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
ALLOW WRITE livello file	autorizza l'accesso in scrittura a tutti i contenuti, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in scrittura a tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in scrittura a tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
DENY WRITE livello file	nega l'accesso in scrittura ai contenuti specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso a una periferica	nega l'accesso in scrittura a tutti i contenuti, nega la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
ALLOW READ/	autorizza l'accesso in lettura e scrittura a	nega l'accesso in lettura e scrittura a	autorizza l'accesso in lettura a tutti i

	FULL ACCESS livello tipo periferica	**NO ACCESS** livello tipo periferica	**ALLOW READ/ DENY WRITE** livello tipo periferica
ALLOW WRITE livello file	tutti i contenuti, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	contenuti, nega l'accesso in scrittura a tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
DENY READ/ DENY WRITE livello file	nega l'accesso in lettura e scrittura ai contenuti specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso a una periferica	nega l'accesso in lettura ai contenuti specificati, nega l'accesso in scrittura a tutti i contenuti, nega la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
ALLOW READ/ DENY WRITE livello file	autorizza l'accesso in lettura a tutti i contenuti, nega l'accesso in scrittura ai contenuti specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in lettura a tutti i contenuti, tranne a quelli specificati, nega l'accesso in scrittura a tutti i contenuti, nega la creazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	autorizza l'accesso in lettura a tutti i contenuti, nega l'accesso in scrittura a tutti i contenuti, nega la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).
DENY READ/ ALLOW WRITE livello file	nega l'accesso in lettura ai contenuti specificati, autorizza l'accesso in scrittura a tutti i contenuti, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in lettura a tutti i contenuti, nega l'accesso in scrittura a tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).	nega l'accesso in lettura ai contenuti specificati, nega l'accesso in scrittura a tutti i contenuti, tranne a quelli specificati, autorizza la creazione, l'eliminazione e la ridenominazione delle cartelle vuote e dei file a zero byte (0).

Nota: se viene impostata l'autorizzazione No Access per un tipo di periferica ed è presente una regola basata sul contenuto che consente l'accesso in scrittura a determinati contenuti per lo stesso tipo di periferica, l'autorizzazione Traverse Folder viene concessa agli utenti per questo tipo di periferica. L'autorizzazione Traverse Folder consente all'utente di spostarsi tra la varie cartelle e visualizzare i file e le cartelle ubicate nelle sottodirectory anche se non dispone dell'autorizzazione di lettura per le cartelle visitate.

Durante l'utilizzo delle regole basate sul contenuto (Content-Aware Rules), considerare quanto segue:

- ***Se le regole basate sul contenuto sono state definite sia per le periferiche sia per i protocolli, tutti i controlli dell'accesso vengono eseguiti in un thread***.
- ***Le regole basate sul contenuto con impostazione Deny (Nega) hanno la priorità su quelle con impostazione Allow (Autorizza) se si applicano agli stessi utenti o agli stessi gruppi***.
- ***Se gli utenti cercano di sovrascrivere un file esistente con un nuovo file per cui non dispongono dell'accesso in scrittura, il vecchio file viene eliminato***.
- ***Se gli utenti cercano di modificare un file per cui non dispongono dell'accesso in scrittura, il file viene eliminato***.
- ***La rimozione non sicura di una periferica può danneggiare il file system e i dati della stessa***.
- ***Se gli utenti tentano di copiare i file per cui non dispongono dell'accesso in scrittura, i file risultano temporaneamente visibili su Esplora risorse o altre applicazioni di gestione file. In realtà, si tratta di file non presenti sulla periferica di destinazione, ubicati nella cache della memoria. Dopo che DeviceLock termina di verificarne il contenuto, questi file vengono rimossi dalla cache***.
- ***Se gli utenti aprono un file da un'unità USB Flash, lo modificano inserendo contenuto per cui non è consentito loro l'accesso in scrittura e tentano di salvare le modifiche, il file viene eliminato***.
- ***La verifica del contenuto dei file è un'operazione che può richiedere molto tempo. Non è possibile rimuovere la periferica in maniera sicura durante l'esecuzione di questa operazione, anche se i file copiati risultano visibili su Esplora risorse o altre applicazioni di gestione dei file. In una situazione del genere, viene visualizzato un messaggio di errore che indica che la periferica è occupata***.
- ***I file copiati di recente possono essere aperti per la lettura solo dopo che DeviceLock ne avrà verificato il contenuto***.
- ***La verifica del contenuto dei file è un'operazione che può richiedere molto tempo. È possibile definire un messaggio di verifica del contenuto da mostrare agli utenti durante l'esecuzione dell'ispezione del contenuto. Per informazioni dettagliate su questo messaggio, consultare la sezione "***Content verification message***" (Messaggio di verifica del contenuto) in "Service Options"***.
- ***Se gli utenti tentano di leggere o scrivere file per cui non dispongono dell'accesso in lettura o scrittura, viene visualizzato un messaggio di blocco di lettura o scrittura basato sul contenuto di DeviceLock, se l'opzione Content-Aware blocked read (o write) message è stata selezionata in Service Options. Per informazioni dettagliate su questi messaggi, consultare le sezioni "***Content-Aware blocked read message***" (Messaggio di blocco di***

lettura basato sul contenuto e "Content-Aware blocked write message***" (Messaggio di blocco di scrittura basato sul contenuto) in "Service Options"***.

Regole basate sul contenuto per le operazioni di copia shadow

Prima di poter utilizzare le Content-Aware Rules (regole basate sul contenuto) per le operazioni di copia shadow, è necessario attivare **Auditing and Shadowing** a livello di tipo periferica. Le regole basate sul contenuto che si applicano alle operazioni di copia shadow filtrano le copie shadow dei file scritte dall'utente.

La seguente tabella fornisce un riepilogo dei diritti di copia shadow che possono essere specificati nelle regole basate sul contenuto.

DIRITTI DI COPIA SHADOW	DESCRIZIONE
Generic: Write	Controlla se eseguire o meno la copia shadow per determinati contenuti scritti su una periferica. Si applica ai tipi di periferica Floppy, iPhone, Removable, Palm e Windows Mobile.
Generic: Print	Controlla se eseguire o meno la copia shadow dei documenti con determinati contenuti inviati alle stampanti. Si applica al tipo di periferica Printer. *DeviceLock estrae e analizza i testi provenienti dai file PostScript, PCL5 e PCL6*.
Encrypted: Write	Determina se eseguire o meno la copia shadow per determinati contenuti scritti su una periferica crittografata. Si applica unicamente al tipo di periferica Removable.
Special Permissions: Write Calendar	Controlla se eseguire o meno la copia shadow per determinati contenuti scritti da un PC sul calendario di un dispositivo mobile. Si applica ai tipi di periferica iPhone, Palm e Windows Mobile.
Special Permissions: Write Contact	Controlla se eseguire o meno la copia shadow per i contatti con determinati contenuti scritti da un PC su un dispositivo mobile. Si applica ai tipi di periferica iPhone, Palm e Windows Mobile.
Special Permissions: Write E-mail	Controlla se eseguire o meno la copia shadow per i messaggi e-mail con determinati contenuti scritti da un PC su un dispositivo mobile. Si applica ai tipi di periferica iPhone, Palm e Windows Mobile. Per l'iPhone, questo diritto controlla la copia shadow delle impostazioni dell'account di posta elettronica ma non dei messaggi, in quanto iTunes non supporta la sincronizzazione dei messaggi.
Special Permissions: Write Attachment	Controlla se eseguire o meno la copia shadow per gli allegati e-mail con determinati contenuti scritti da un PC su un dispositivo Windows Mobile o Palm.
Special Permissions: Write Favorite	Controlla se eseguire o meno la copia shadow per i favoriti con determinati contenuti scritti da un PC su un dispositivo Windows Mobile o iPhone.

DIRITTI DI COPIA SHADOW	DESCRIZIONE
Special Permissions: Write File	Controlla se eseguire o meno la copia shadow per i file con determinati contenuti scritti da un PC su un dispositivo mobile. Si applica ai tipi di periferica iPhone, Palm e Windows Mobile.
Special Permissions: Write Media	Controlla se eseguire o meno la copia shadow dei file multimediali con determinati contenuti scritti utilizzando Windows Media Player da un PC su un dispositivo Windows Mobile e dei file multimediali con determinati contenuti scritti da un PC su un dispositivo Palm o iPhone.
Special Permissions: Write Backup	Controlla se eseguire o meno la copia shadow per i dati di backup dell'iPhone con determinati contenuti scritti da un PC su un dispositivo iPhone.
Special Permissions: Write Note	Controlla se eseguire o meno la copia shadow per le note con determinati contenuti scritte da un PC su un dispositivo mobile. Si applica ai tipi di periferica iPhone, Palm e Windows Mobile.
Special Permissions: Write Pocket Access	Controlla se eseguire o meno la copia shadow per i database di Pocket Access con determinati contenuti scritti da un PC su un dispositivo Windows Mobile.
Special Permissions: Write Task	Controlla se eseguire o meno la copia shadow per le attività con determinati contenuti scritte da un PC su un dispositivo mobile. Si applica ai tipi di periferica Palm e Windows Mobile.
Special Permissions: Write Expense	Controlla se eseguire o meno la copia shadow per i dati dell'applicazione Palm Expense con determinati contenuti scritti da un PC su un dispositivo Palm.
Special Permissions: Write Document	Controlla se eseguire o meno la copia shadow per i documenti di Palm con determinati contenuti scritti da un PC su un dispositivo Palm.
Special Permissions: Write Unidentified Content	Controlla se eseguire o meno la copia shadow per tutti gli altri dati senza categoria con determinati contenuti scritti da un PC su un dispositivo Windows Mobile.

Nota: i diritti di copia shadow generica specificati per il tipo di periferica Removable si applicano solo alle periferiche non crittografate. I diritti di copia shadow crittografata specificati per il tipo di periferica Removable si applicano solo alle periferiche crittografate. Per specificare i diritti di copia shadow per entrambi i tipi di periferica Removable (crittografata e non crittografata), occorre specificare entrambi i diritti di copia shadow, generica e crittografata.

Configurazione delle impostazioni di rilevamento del contenuto

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto, che consentono di definire centralmente i tipi di contenuto per cui verificare l'accesso. I gruppi di contenuto specificano i criteri di filtraggio del contenuto che verranno utilizzati per selezionare i dati a cui applicare le regole.

Tutti i gruppi di contenuto sono memorizzati nel database dei contenuti. Per le periferiche e i protocolli viene utilizzato lo stesso database dei contenuti. Il database dei contenuti, che fa parte dei criteri di DeviceLock Service, viene salvato in un file XML contenente le impostazioni del servizio. Questo file può essere creato utilizzando DeviceLock Management Console, DeviceLock Service Settings Editor e DeviceLock Group Policy Manager.

Sono disponibili diversi tipi di gruppi di contenuto: File Type Detection (Rilevamento tipo file), Keywords (Parole chiave), Pattern (Motivi), Document Properties (Proprietà documenti) e Complex (Complessi). La sezione sottostante descrive i gruppi e spiega come utilizzarli.

Gruppi di contenuto File Type Detection (Rilevamento tipo file)

I gruppi File Type Detection vengono utilizzati per controllare l'accesso ai file in base ai tipi di file. Questi gruppi contengono le definizioni del tipo di file inclusi nei gruppi. Una definizione del tipo di file è composta da due proprietà: l'estensione del file (ad esempio DOC) e la descrizione (ad esempio documento di Microsoft Word). Quando viene applicata una regola basata su un gruppo File Type Detection, la regola viene applicata a tutti i tipi di file inclusi nel gruppo.

Definendo le regole in base ai gruppi File Type Detection, è ad esempio possibile autorizzare la lettura e negare la scrittura dei documenti Word provenienti dalle unità Floppy a determinati utenti o gruppi. È possibile negare l'accesso in lettura a tutti i file eseguibili provenienti dalle periferiche Removable, DVD/CD-ROM e Floppy, ma autorizzare l'accesso in scrittura a tutti i tipi di file per i dispositivi Removable e Floppy. È inoltre possibile impostare la copia shadow solo per i documenti Word, Excel e PDF.

DeviceLock include 34 gruppi File Type Detection predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
Archives	MS Outlook & Outlook Express
Audio, Video & Flash	MS PowerPoint
BlackBerry	MS Project
Common Object File Format (COFF)	MS Publisher
Database	MS Visio
Executable	MS Windows Installer
Fax Documents	MS Windows Memory Dump
FileMaker Pro	MS Word
Fonts	MS Works
Help Files	OpenOffice, StarOffice, OpenDocument, etc.
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
Lotus SmartSuite	QuickBooks, Quicken, TurboTax & etc.
MS Access	Rich Text Format
MS Excel	Security Certificates

GRUPPI DI CONTENUTO PREDEFINITI	
MS InfoPath MS Money MS OneNote	Text, HTML & XML Virtual Machines WordPerfect Office

Nota: le regole basate sul contenuto supportano i formati Word To Go, Sheet To Go e Slideshow To Go per i dispositivi Palm. Il formato Word To Go è incluso nei gruppi di contenuto incorporati MS Word e Rich Text Format, il formato Sheet To Go è incluso nel gruppo di contenuto incorporato MS Excel e il formato Slideshow To Go è incluso nel gruppo di contenuto incorporato MS PowerPoint.

I file Microsoft Word, RTF (Rich Text Format), Excel e PowerPoint possono essere trasferiti su un dispositivo Palm utilizzando l'applicazione Documents To Go. L'applicazione Documents To Go converte questi file in formati speciali: i file Word e RTF in formato Word To Go, i file Excel in formato Sheet To Go e i file PowerPoint in formato Slideshow To Go. I file convertiti vengono scaricati automaticamente sul dispositivo Palm quando l'utente esegue la sincronizzazione.

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare le definizioni del tipo di file incluse nei gruppi File Type Detection incorporati, ma non modificarle né eliminarle. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione "Visualizzazione dei gruppi di contenuto incorporati".

Creazione di gruppi di contenuto File Type Detection personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto File Type Detection personalizzati consentono di specificare qualsiasi tipo di file da includere nello stesso gruppo, in base alle esigenze specifiche di ciascun utente.

Si supponga di voler garantire a determinati utenti l'accesso ai documenti Word, Excel e PDF e ai file di grafica. Per farlo, occorre innanzitutto creare un nuovo gruppo di contenuto che rappresenti questi tipi di documenti. In seguito, si può definire una regola basata su questo gruppo di contenuto personalizzato.

Per creare un gruppo File Type Detection personalizzato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

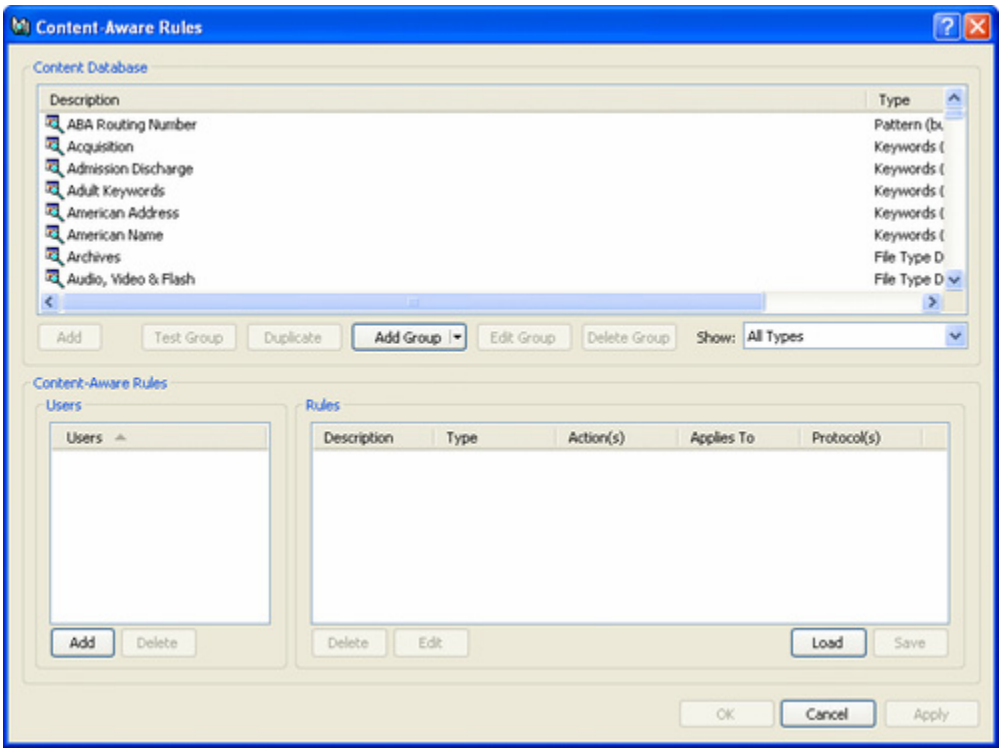
   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.

b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

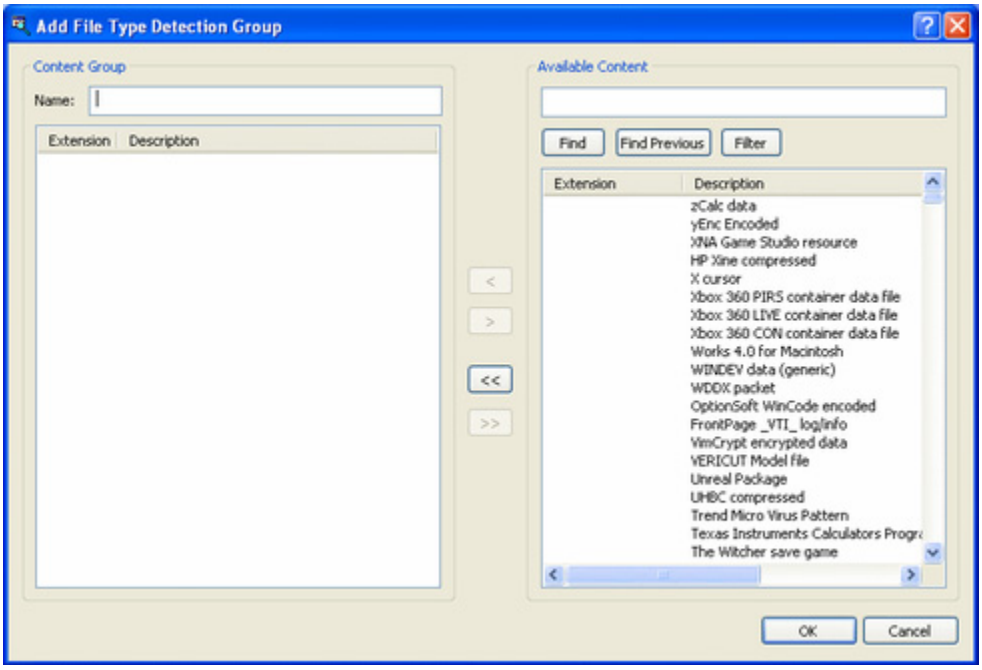
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **File Type Detection**.

   Viene visualizzata la finestra di dialogo Add File Type Detection Group.



5. Nel riquadro sinistro della finestra di dialogo **Add File Type Detection Group**, sotto **Content group**, digitare il nome del nuovo gruppo di contenuto nella casella **Name**.

   Nota: un nuovo gruppo di contenuto non può avere lo stesso nome di un gruppo di contenuto esistente.

6. Nel riquadro destro della finestra di dialogo **Add File Type Detection Group**, sotto **Available Content**, selezionare il tipo di file da aggiungere al nuovo gruppo di contenuto, quindi fare clic sul pulsante della freccia singola a sinistra <.

   È possibile selezionare più tipi di file tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui tipi di file.

   Per rimuovere singoli tipi di file dal gruppo di contenuto, utilizzare il pulsante della freccia singola a destra >. Per aggiungere/rimuovere simultaneamente tutti i tipi di file disponibili al/dal gruppo di contenuto, utilizzare il pulsante della doppia freccia a sinistra << o della doppia freccia a destra >>.

   Nota: è possibile eseguire ricerche nel database di contenuto disponibile per tipi di file specifici tramite l'estensione o la descrizione. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?) per cercare un gruppo specifico di tipi di file. Per trovare un tipo di file o un gruppo di tipi di file specifico, sotto **Available Content** digitare un'estensione o una descrizione (con o senza caratteri jolly) nella stringa di ricerca, quindi fare clic su **Find**. Per applicare un filtro ai tipi di file, fare clic su **Filter**. Per rimuovere il filtro, applicarlo a una stringa vuota.

   Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità.

7. Fare clic su **OK** per chiudere la finestra di dialogo **Add File Type Detection Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo

Content-Aware Rules.

Gruppi di contenuto Keywords (Parole chiave)

I gruppi Keywords vengono utilizzati per controllare l'accesso ai file in base alla presenza di determinati termini o frasi in un documento.

Definendo le regole basate sui gruppi Keywords, ad esempio, è possibile autorizzare l'accesso in lettura a tutti i documenti che contengono le frasi "Top Secret" e "Solo per uso ufficiale" dalle periferiche Removable, Floppy e DVD/CD-ROM e negare l'accesso in scrittura alle periferiche Removable e Floppy per tali documenti. È inoltre possibile impostare la copia shadow solo per i documenti che contengono le frasi "Top Secret" e "Solo per uso ufficiale".

DeviceLock include 157 gruppi Keywords predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss
Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property
American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation
Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital
Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses

GRUPPI DI CONTENUTO PREDEFINITI

Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver's License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medicinal Active Substances
FITS Date & Time	Russian: Medicinal Drugs
FITS File Checksum	Russian: Noncompliant
FITS File Descriptors	Russian: Passwords and Access Codes
FITS Hierarchical file grouping	Russian: Physical Security
FITS Instrumentorum	Russian: Prices
FITS Non-standard	Russian: Project Documentation
FITS Observations	Russian: Project Names
FITS Standard	Russian: Project Versions
Gambling	Russian: Projects Release Date
Grades	Russian: Technology
HCFA (CMS) 1500 Form	Russian: User Names
HIPAA - Diseases	Russian: Working Conditions
HIPAA HCPCS	Sales Forecast
HIPAA ICD9	Sarbanes-Oxley Sensitive
HIPAA NDC Classes	Security
HIPAA NDC Dosages	Security Agencies
HIPAA NDC Listing	Sensitive Disease
HIPAA NDC Routes	Sexual Language
Illegal Drugs	Social Security
Innovations	SPAM
Internet Slang Abbreviations	Sports
Investments	Staff Training
Java Source Code	Substance Abuse
Market Development	Suspicious Activity Report
Medical Diagnosis	Technology
Medical Record Numbers	UBO4 Form
MEMO	US Birth Date
Network Security	US Birth Place
Partner Names	US Expiry Date
Password	User Name
Payments	VB Source Code
PCI GLBA	Violence
Perl Source Code	Weapon Keywords
Price List	Wire Transfer
Prices	Working Conditions
Pro Earnings	

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare le parole chiave incluse nei gruppi Keywords incorporati, ma non modificarle né eliminarle. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione "Visualizzazione dei gruppi di contenuto incorporati".

Creazione di gruppi Keywords (Parole chiave) personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto Keywords personalizzati consentono di specificare qualsiasi tipo di parola chiave da includere nello stesso gruppo, in base alle esigenze specifiche di ciascun utente.

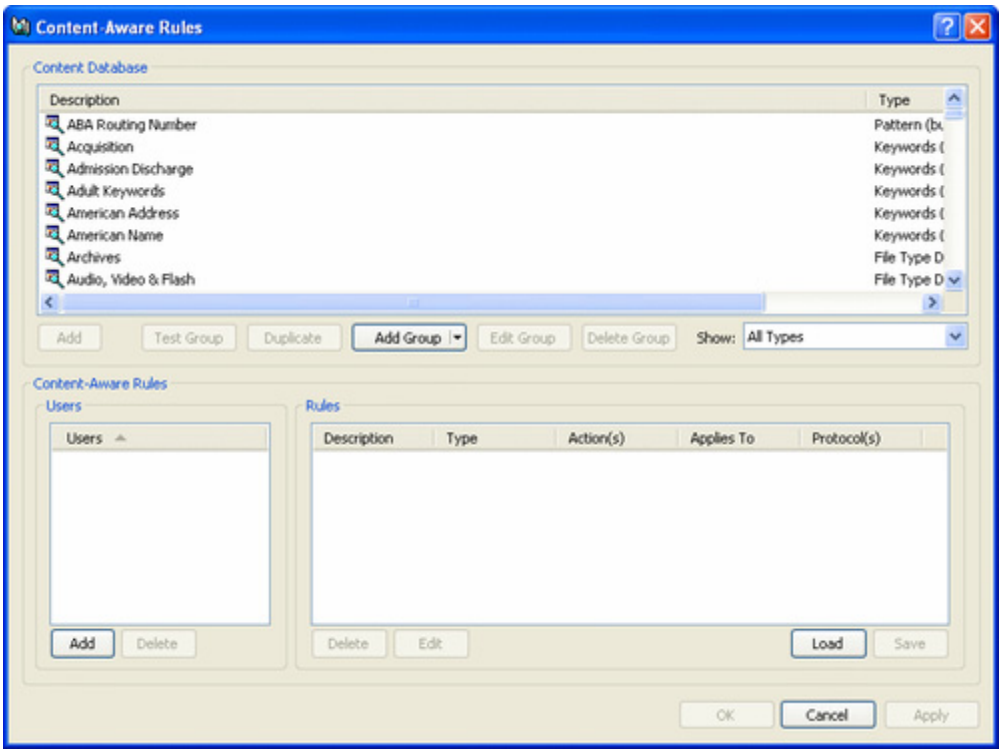
Per creare un gruppo Keywords personalizzato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

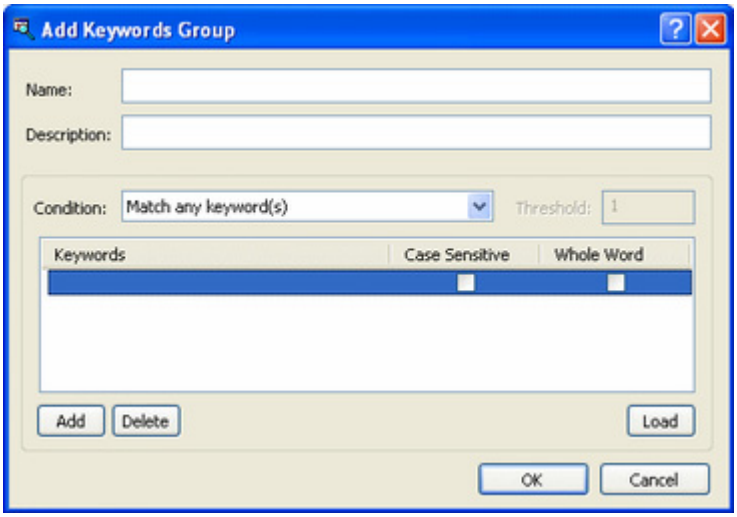
   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Keywords**.

   Viene visualizzata la finestra di dialogo Add Keywords Group.



5. Nella finestra di dialogo **Add Keywords Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Condition:	Specificare le condizioni delle regole di attivazione associate a questo gruppo di contenuto. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Condition**: • **Match any keyword(s)**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che una qualsiasi delle parole chiave specificate viene rilevata tra i dati di testo. • **Match all keyword(s)**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che tutte le parole chiave specificate vengono rilevate tra i dati di testo. • **Only when combined score exceeds (or equal to) threshold**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero totale (la somma) delle occorrenze di tutte le parole chiave rilevate tra i dati di testo raggiunge o supera la soglia delle occorrenze di parole chiave.
Threshold	Specificare il numero di occorrenze delle parole chiave della soglia. Il numero deve essere compreso tra 0 e 65535. Se è stata specificata l'opzione **Only when combined score exceeds (or equal to) threshold**, questa proprietà richiede un valore.
Keywords	Specificare le parole e le frasi che devono verificarsi tra i dati di testo. Fare doppio clic sotto **Keywords** per immettere una parola chiave o una frase.
Case Sensitive	Determinare il tipo di distinzione tra maiuscole e minuscole delle parole chiave. Selezionare la casella di controllo **Case Sensitive** per attivare la distinzione tra maiuscole e minuscole delle parole chiave (ad esempio, le parole "test" e "Test" verranno trattate come due parole chiave distinte). Deselezionare la casella di controllo **Case Sensitive** per disattivare la distinzione tra maiuscole e minuscole delle parole chiave (ad esempio, le parole "test" e "Test" verranno considerate come un'unica parola chiave).
Whole Word	Specificare le opzioni di corrispondenza con le parole chiave. Selezionare la casella di controllo **Whole Word** per specificare l'opzione di corrispondenza esatta (consente di trovare una corrispondenza esatta con la parola chiave). Deselezionare la casella di controllo **Whole Word** per specificare l'opzione di corrispondenza più estesa (consente di trovare tutte le varianti grammaticali della parola chiave).
Weight	Specificare il grado di importanza di ciascuna parola chiave o frase. Questo valore viene utilizzato per contare il numero di occorrenze delle parole chiave specificate tra i dati di testo. Se è stata specificata l'opzione **Only when combined score exceeds (or equal to) threshold**, questa proprietà richiede un valore.

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	Valori possibili: **Heavy**, **Above Normal**, **Normal** (valore predefinito), **Below Normal**, **Light**. Interpretazione dei valori: **Heavy** indica che ciascuna ocorrenza di parola chiave viene contata come tre occorrenze. Si tratta del valore più elevato. **Above normal** indica che ciascuna ocorrenza di parola chiave viene contata come due occorrenze. **Normal** indica che ciascuna ocorrenza di parola chiave viene contata come un'occorrenza. **Below normal** indica che due occorrenze di parola chiave vengono contate come un'occorrenza. **Light** indica che tre occorrenze di parola chiave vengono contate come un'occorrenza. Si tratta del valore più basso.
Add	Specificare le parole chiave e le frasi. Fare clic su **Add** per immettere una parola chiave o una frase.
Delete	Eliminare una parola chiave. Per farlo, selezionare la parola chiave che si desidera eliminare e fare clic su **Delete**. È possibile selezionare più parole chiave tenendo premuto il tasto MAIUSC o CTRL e facendo clic sulle parole chiave.
Load	Importare un elenco di parole chiave da un file di testo delimitato da tabulazione.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Keywords Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Pattern (Motivi)

I gruppi Pattern consentono di controllare l'accesso ai file di testo utilizzando motivi di testo descritti dalle espressioni comuni Perl. I motivi rappresentano uno strumento efficace e flessibile per eseguire il rilevamento automatico di contenuti potenzialmente riservati (ad esempio numeri di carta di credito e di codice fiscale, indirizzi e-mail e numeri di telefono) all'interno dei documenti.

Per ulteriori informazioni sulla creazione e l'utilizzo delle espressioni comuni Perl, consultare le sezioni Guida introduttiva alle espressioni comuni Perl e Guida alle espressioni comuni Perl.

Definendo le regole in base ai gruppi Pattern, è ad esempio possibile negare la scrittura dei documenti contenenti numeri di carta di credito sulle periferiche Removable e Floppy. È

inoltre possibile disattivare la copia shadow dei documenti che non contengono numeri di carta di credito.

DeviceLock include 45 gruppi Pattern predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
ABA Routing Number	Russian: Main State Registration Number
BIC (ISO 9362)	Russian: Motorcycle Numbers
Canadian Social Insurance Number	Russian: Passport
Credit Card Number	Russian: Pension Insurance Number
Email Address	Russian: Post Code
European VAT Number	Russian: Taxpayer Identification Number
GPS Data (RMC String)	Russian: Telephone Number
IBAN	Russian: Trailer Numbers
International Telephone Number	Russian: Vehicle Registration Document
IP Address	SQL Queries
ISO Date	TCP/UDP Port Number
MAC Address	Time (12/24h)
Microsoft Windows Product Key	UK National Insurance Number
Russian: Address	UK Phone Number
Russian: Auto Insurance Number	UK Post Code
Russian: Bank Account Number	UK Tax Code
Russian: BIC	Uniform Resource Locator (URL)
Russian: Car Numbers	US Date
Russian: Classification of Economic Activities	US Phone Number
	US Social Security Number
Russian: Classification of Enterprises and Organizations	US Zip Code
	VIN
Russian: Driver’s License Number	
Russian: Health Insurance Number	
Russian: International Passport	

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare i motivi di espressioni comuni nei gruppi Pattern incorporati, ma non modificarli né eliminarli. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione “Visualizzazione dei gruppi di contenuto incorporati”.

Creazione di gruppi Pattern (Motivi) personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto Pattern personalizzati consentono di specificare qualsiasi motivo da utilizzare per identificare le informazioni riservate nei documenti.

Per creare un gruppo Pattern personalizzato

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

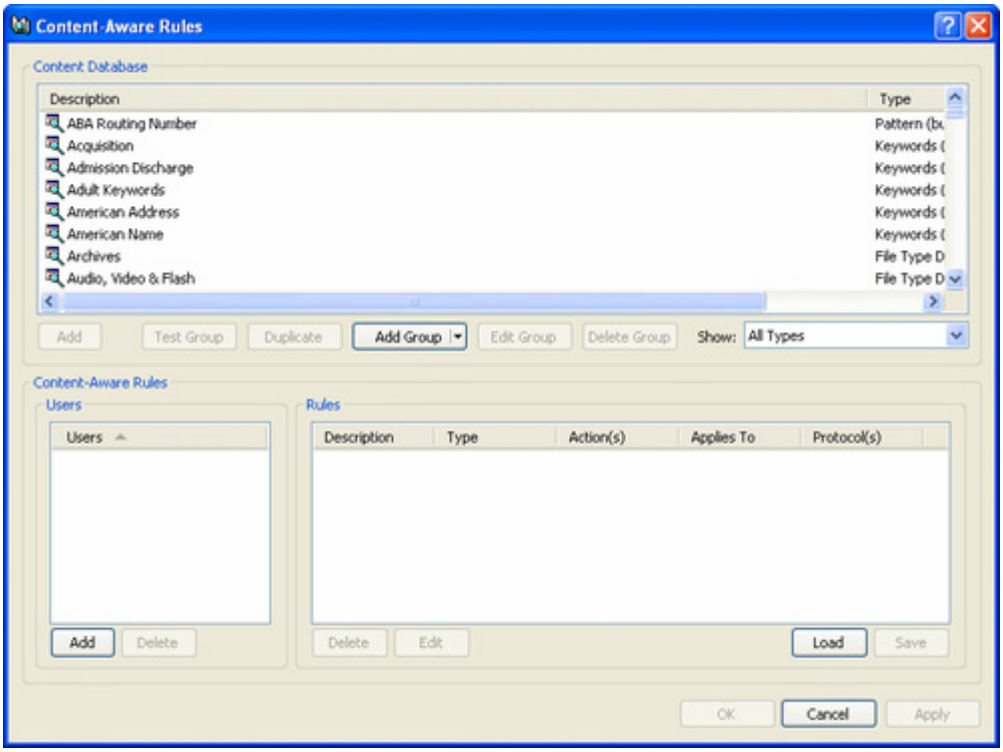
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.

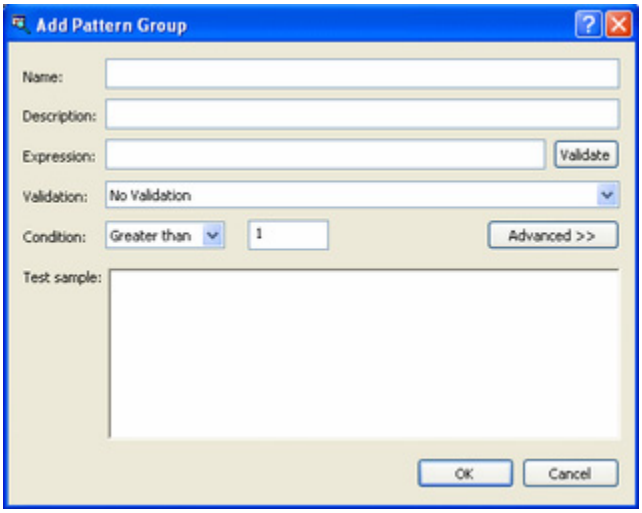
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Pattern**.

   Viene visualizzata la finestra di dialogo Add Pattern Group.



5. Nella finestra di dialogo **Add Pattern Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Expression	Specificare un motivo creando un'espressione comune. Per informazioni sulla creazione delle espressioni comuni Perl, consultare le sezioni Guida introduttiva alle espressioni comuni Perl e Guida alle espressioni comuni Perl.
Validate	Verificare la sintassi dell'espressione comune.
Validation	Eseguire la convalida delle corrispondenze potenziali restituite dall'espressione comune. Sono disponibili le seguenti opzioni: **No validation** (opzione predefinita), **ABA Routing Number**, **Canadian Social Insurance Number**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Date, Date (ISO)**, **Email Address**, **European VAT Number**, **IBAN**, **IP Address**, **LUHN Checksum**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations**, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social**

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	Security Number.
Condition:	Specificare le condizioni delle regole di attivazione associate a questo gruppo di contenuto. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Condition**: • **Less than or =** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è inferiore o uguale al numero specificato. • **Equal to** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è uguale al numero specificato. • **Greater than or =** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è superiore o uguale al numero specificato. • **Between** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è compreso nell'intervallo specificato.
Advanced	Verificare rapidamente il motivo dell'espressione comune su dati campione. Fare clic su **Advanced** per visualizzare o nascondere la casella **Test sample.**
Test sample	Inserire una stringa campione e visualizzare il risultato. DeviceLock supporta l'evidenziazione a colori in tempo reale dei risultati del test. Tutte le corrispondenze vengono evidenziate in verde, mentre le stringhe che non corrispondono al motivo vengono evidenziate in rosso.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Pattern Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Document Properties (Proprietà documenti)

I gruppi Document Properties consentono di controllare l'accesso ai file in base a proprietà dei file come nome e dimensione file, ecc. È inoltre possibile utilizzare un gruppo di contenuto Document Properties per controllare l'accesso a documenti e archivi protetti da password e immagini di testo.

Nota: la logica AND viene applicata a tutte le proprietà di file specificate in un gruppo Document Properties. Se, ad esempio, si desidera controllare l'accesso ai file di dimensioni superiori a 5 megabyte (MB) e ai documenti e agli archivi protetti da password, è necessario creare due gruppi Document Properties separati: uno per i file di dimensioni superiori a 5 MB e l'altro per i documenti e

gli archivi protetti da password. Se queste proprietà di file vengono specificate nello stesso gruppo Document Properties e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà i documenti e gli archivi protetti da password di dimensioni superiori a 5 MB.

Definendo le regole basate sui gruppi Document Properties, ad esempio, è possibile autorizzare l'accesso in lettura per tutti i documenti di dimensioni superiori a 1 MB dalle periferiche Removable, Floppy e DVD/CD-ROM e negare l'accesso in scrittura alle periferiche Removable e Floppy per tali documenti. È inoltre possibile autorizzare la copia shadow solo per i documenti di dimensione superiore a 5 MB.

Non sono presenti gruppi di contenuto Document Properties predefiniti (incorporati). La seguente procedura descrive come creare gruppi Document Properties personalizzati.

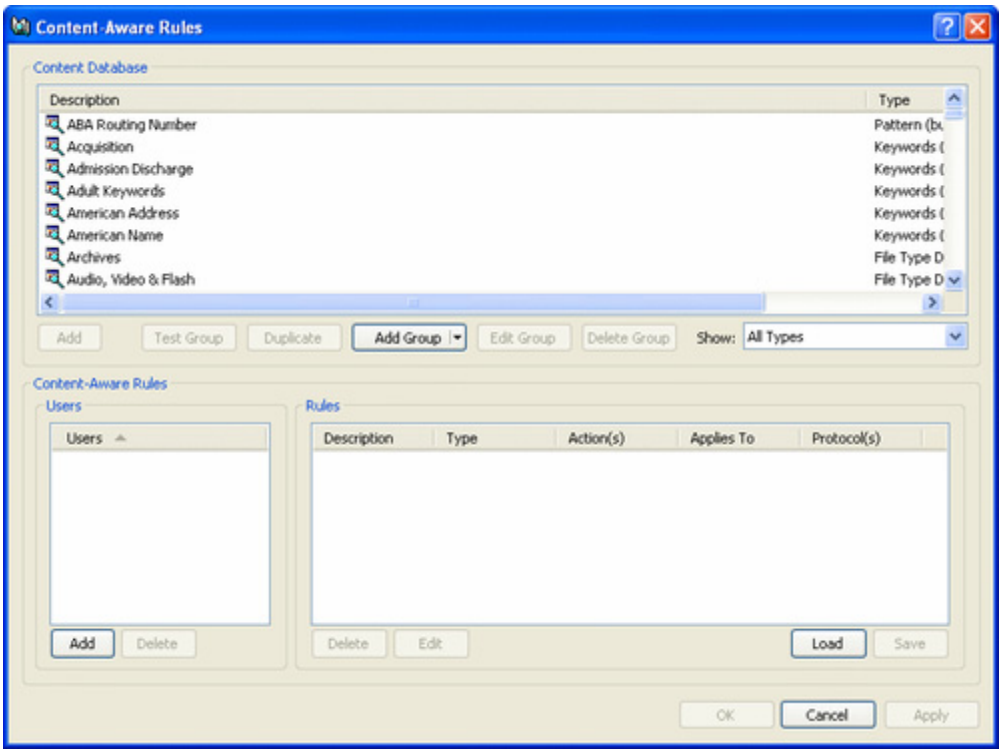
Per creare un gruppo Document Properties (Proprietà documenti)

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Service Settings Editor:
    a) Aprire DeviceLock Service Settings Editor.
    b) Nella struttura della console, espandere **DeviceLock Service**.

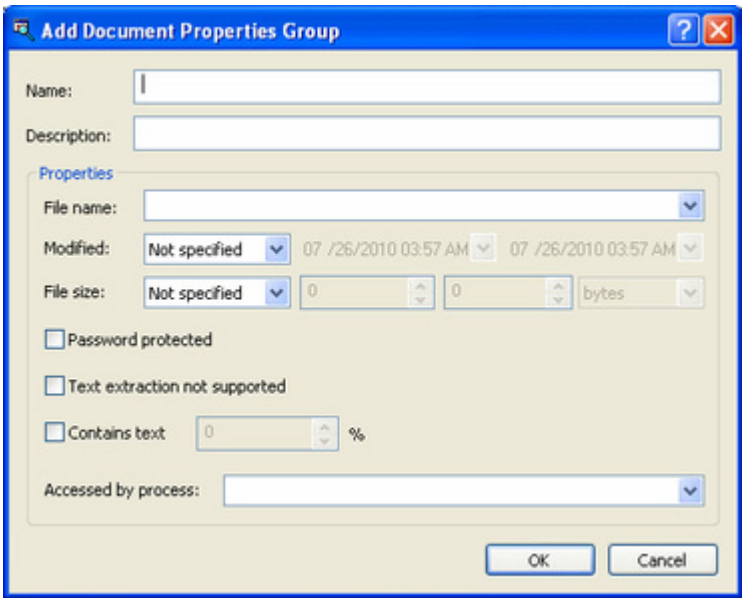
    Se si utilizza DeviceLock Group Policy Manager:
    a) Aprire Group Policy Object Editor.
    b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
    - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
      - OPPURE -
    - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

    Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Document Properties**.

   Viene visualizzata la finestra di dialogo Add Document Properties Group.



5. Nella finestra di dialogo **Add Document Properties Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
File name	Specificare i nomi di file. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?). Ad esempio, digitare ***.txt** per specificare tutti i file con estensione .txt. I nomi di file multipli vanno separati da una virgola da un punto e virgola (;), ad esempio ***.doc; *.docx**. *Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere*. **Nota:** per i dati shadow acquisiti dalle periferiche di tipo stampante, il valore del nome file specificato è comparato con i nomi indicati nella colonna **File Name** del visualizzatore del registro shadow.
Modified	Specificare l'ultima data/ora di modifica del file. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Modified**: • **Not specified** (opzione predefinita) • **Before than** indica che la data/ora di modifica del file deve essere precedente alla data/ora specificata. • **After than** indica che la data/ora di modifica del file deve essere posteriore alla data/ora specificata. • **Between** indica che la data/ora di modifica del file deve rientrare nell'intervallo di date/ore specificato. • **Not older than** indica che la data/ora di modifica del file non deve essere antecedente al numero specificato di secondi, minuti, giorni, settimane, mesi e anni. • **Older than** indica che la data/ora di modifica del file deve essere antecedente al numero specificato di secondi, minuti, giorni, settimane, mesi e anni.
File size	Specificare la dimensione del file in byte, kilobyte, megabyte, gigabyte o terabyte. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **File size**: • **Not specified** (opzione predefinita) • **Equal to** indica che la dimensione del(i) file deve corrispondere alla dimensione specificata. • **Less than** indica che la dimensione del(i) file deve essere inferiore alla dimensione specificata. • **More than** indica che la dimensione del(i) file deve essere superiore alla dimensione specificata. • **Between** indica che la dimensione del(i) file deve rientrare nell'intervallo specificato.
Password protected	Rilevare e controllare l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx) protetti da password. Se viene selezionata la casella di controllo **Password**

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	protected per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office protetti da password. Deselezionare la casella di controllo **Password protected** se non si desidera rilevare e controllare l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office protetti da password. Per informazioni sui formati di archivio supportati, consultare la descrizione della funzionalità "Ispezione di file all'interno di archivi".
Text extraction not supported	Controllare l'accesso ai formati di file non supportati. Se viene selezionata la casella di controllo **Text extraction not supported** per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà l'accesso a tutti i file di formati non supportati. Per visualizzare l'elenco completo dei file supportati, consultare la sezione "Estensione delle funzionalità di DeviceLock con ContentLock e NetworkLock".
Contains text	Rilevare e controllare l'accesso alle immagini in base della presenza di testo o meno all'interno di queste ultime. Se viene selezionata la casella di controllo **Contains text** per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto e al gruppo di contenuto incorporato Images, CAD & Drawing (File Type Detection: Rilevamento tipo file), la regola verificherà la presenza di testo nei file di immagine supportati e controllerà l'accesso alle immagini di testo. Deselezionare la casella di controllo **Contains text** se non si desidera rilevare e controllare l'accesso alle immagini di testo. Per informazioni sui file di immagine supportati, consultare la descrizione della funzionalità "Rilevamento di testo nelle immagini". Se viene selezionata la casella di controllo **Contains text**, specificare la quantità di testo contenuta nelle immagini. La quantità di testo viene espressa in termini percentuali rispetto all'area totale dell'immagine. Ad esempio, se il testo occupa la metà dell'immagine, la quantità di testo equivale al 50%. Se un'immagine contiene solo testo, la quantità di testo equivale al 100%. **Nota:** l'opzione **Contains text** si applica anche agli altri formati di file supportati. In questo caso, la percentuale indica il rapporto tra la dimensione del testo in caratteri e la dimensione del file in byte.
Accessed by process	Specificare il nome del processo che accede al file del documento. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?). I nomi di processi multipli vanno separati da un punto e virgola (;), ad esempio **explorer.exe; notepad.exe**.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Document Properties Group**.

Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Complex (Complessi)

I gruppi Complex ricorrono alle espressioni booleane per selezionare i documenti per cui si desidera controllare l'accesso. Questi gruppi possono includere qualsiasi combinazione di gruppi di contenuto incorporati o personalizzati (File Type Detection, Keywords, Pattern e Document Properties) associati a qualsiasi numero di operatori logici standard. Ciascun gruppo di contenuto viene trattato come singolo criterio di filtro che può essere incluso nell'espressione booleana dell'utente. Utilizzando più gruppi di contenuto, è possibile creare filtri complessi al fine di identificare il contenuto riservato dei documenti.

La seguente tabella include gli operatori logici in ordine di preferenza, dal più elevato al più basso

OPERATORE	SIGNIFICATO
NOT	Negazione logica di un criterio di filtro
AND	Entrambi i criteri di filtro vanno applicati
OR	Può essere applicato l'uno o l'altro criterio di filtro

È possibile utilizzare parentesi per modificare la precedenza degli operatori e forzare la valutazione di alcune parti di un'espressione prima di altre. I criteri nidificati inclusi tra parentesi vengono valutati nell'ordine dall'interno verso l'esterno. Sono supportati più livelli di nidificazione. Un gruppo complesso può contenere un massimo di 30 gruppi di contenuto.

Non sono presenti gruppi di contenuto Complex predefiniti (incorporati). La seguente procedura descrive come creare gruppi Complex personalizzati.

Per creare un gruppo Complex (Complessi)

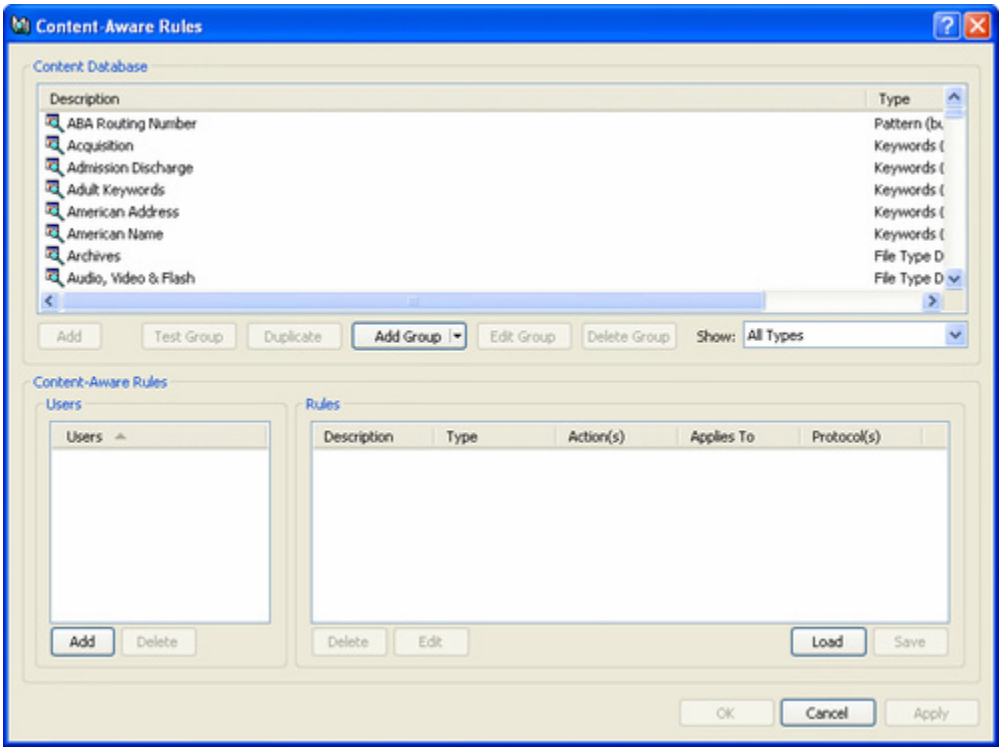
1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Service Settings Editor:
    a) Aprire DeviceLock Service Settings Editor.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Group Policy Manager:
    a) Aprire Group Policy Object Editor.
    b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.

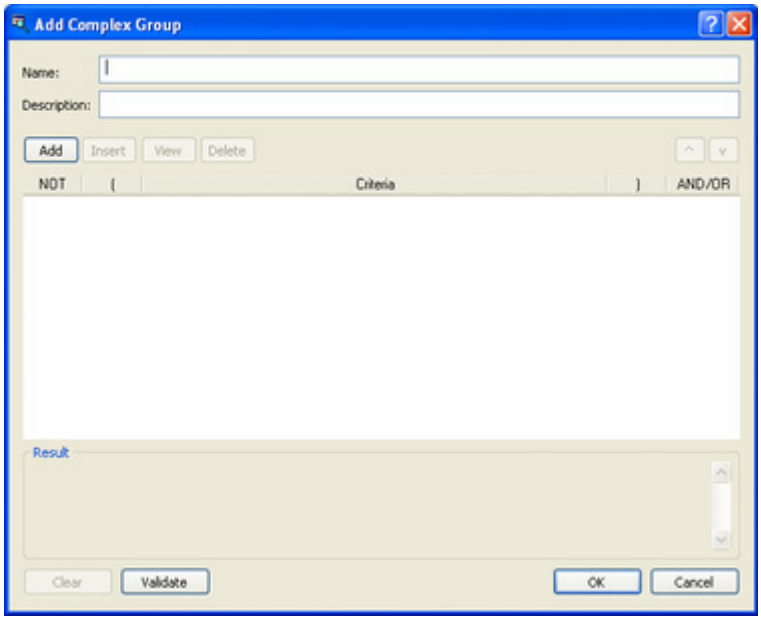
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Complex**.

   Viene visualizzata la finestra di dialogo Add Complex Group.



5. Nella finestra di dialogo **Add Complex Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Add	Aggiungere i gruppi di contenuto desiderati selezionandoli dal database dei contenuti. Per farlo, fare clic su **Add** per aprire la finestra di dialogo **Content Groups**. Nella finestra di dialogo **Content Groups**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **OK**. *È possibile selezionare più gruppi di contenuto tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui gruppi.* *Per visualizzare le informazioni su un gruppo di contenuto, selezionare il gruppo desiderato e fare clic su View Group.* *I gruppi di contenuto aggiunti vengono visualizzati nella colonna Criteria della finestra di dialogo Add Complex group. Ciascun gruppo di contenuto aggiunto viene trattato come singolo criterio di filtro che può essere incluso nell'espressione booleana dell'utente.*
Insert	Inserire uno dei gruppi di contenuto inclusi nel database dei contenuti prima del gruppo correntemente selezionato nella colonna **Criteria**. Per farlo, fare clic su **Insert** per aprire la finestra di dialogo **Content Groups**. Nella finestra di dialogo **Content Groups**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **OK**.
View	Visualizzare informazioni sul gruppo correntemente selezionato nella colonna **Criteria**.

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Delete	Eliminare il gruppo selezionato dalla colonna **Criteria**.
NOT	Associare a ciascun gruppo di contenuto selezionato un operatore logico NOT. Per farlo, selezionare il gruppo desiderato nella colonna **Criteria**, quindi scegliere la casella di controllo pertinente nella colonna **Not**.
AND/OR	Associare a ciascun gruppo di contenuto selezionato l'operatore logico AND od OR. Per farlo, selezionare il gruppo desiderato nella colonna **Criteria**, quindi fare clic su **AND** od **OR** nell'elenco appropriato nella colonna **AND/OR**.
Clear	Cancellare l'elenco corrente dei gruppi di contenuto nella colonna **Criteria**.
Validate	Convalidare l'espressione. Se l'espressione è stata definita in maniera incorretta (ad esempio, una parentesi aperta non è stata accompagnata da una parentesi chiusa), viene visualizzato un messaggio di errore.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Complex Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Visualizzazione dei gruppi di contenuto incorporati

È possibile visualizzare tutti i gruppi di contenuto incorporati, ma non modificarli né eliminarli.

Per visualizzare un gruppo di contenuto incorporato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
  - OPPURE -
- Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo incorporato da visualizzare, quindi fare clic su **View Group**.

Duplicazione dei gruppi di contenuto incorporati

Non è possibile modificare i gruppi di contenuto incorporati, mentre si possono creare e utilizzare copie modificabili di questi ultimi (duplicati) in base alle esigenze della propria organizzazione.

Per duplicare un gruppo di contenuto incorporato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare il gruppo di contenuto incorporato che si desidera duplicare, quindi fare clic su **Duplicate**.
5. Nella finestra di dialogo visualizzata, apportare le modifiche desiderate al gruppo di contenuto, quindi fare clic su **OK**.

Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Modifica ed eliminazione dei gruppi di contenuto personalizzati.

È possibile modificare o eliminare i gruppi di contenuto personalizzati in qualsiasi momento.

Per modificare o eliminare un gruppo di contenuto personalizzato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.
4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo di contenuto da modificare o eliminare.
5. Fare clic su **Edit Group** per modificare il gruppo di contenuto selezionato. Nella finestra di dialogo visualizzata, apportare le modifiche desiderate, quindi fare clic su **OK**.

   - OPPURE -

   Fare clic su **Delete Group** o premere il tasto CANC per eliminare il gruppo di contenuto selezionato.
6. Nella finestra di dialogo **Content-Aware Rules**, fare clic su **OK** o **Apply** per applicare le modifiche.

Verifica dei gruppi di contenuto

È possibile verificare qualsiasi gruppo di contenuto incorporato o personalizzato per vedere se i file specificati corrispondono allo stesso. Grazie a questo tipo di test, è possibile verificare il rispetto dei propri requisiti aziendali specifici da parte delle regole create in base ai gruppi di contenuto.

Per verificare un gruppo di contenuto

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.
4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo incorporato da verificare, quindi fare clic su **Test Group**.

   È possibile verificare un solo gruppo alla volta.

   Viene visualizzata la finestra di dialogo Open.
5. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da utilizzare per verificare il gruppo di contenuto specificato.
6. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
7. Fare clic sul file, quindi scegliere **Open**.

   Viene visualizzata la finestra di messaggio Result. Se il file corrisponde al gruppo di contenuto specificato, nella finestra di messaggio Result viene visualizzata la seguente frase: "Selected file matches with the group". Se il file non corrisponde al gruppo di contenuto specificato, nella finestra di messaggio Result viene visualizzata la seguente frase: "Selected file does not match with the group".

   Durante la verifica, la console non risponde ai comandi (si blocca).

Gestione delle regole basate sul contenuto

La gestione delle Content-Aware Rules (regole basate sul contenuto) include le seguenti attività:

- Definizione delle regole basate sul contenuto
- Modifica delle regole basate sul contenuto
- Copia delle regole basate sul contenuto
- Esportazione e importazione delle regole basate sul contenuto
- Rimozione della definizione delle regole basate sul contenuto
- Eliminazione delle regole basate sul contenuto

È possibile gestire le regole basate sul contenuto utilizzando DeviceLock Management Console, DeviceLock Group Policy Manager o DeviceLock Service Settings Editor.

Definizione delle regole basate sul contenuto

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto incorporati o personalizzati. Per informazioni dettagliate su questi gruppi, consultare la sezione "Configurazione delle impostazioni di rilevamento del contenuto".

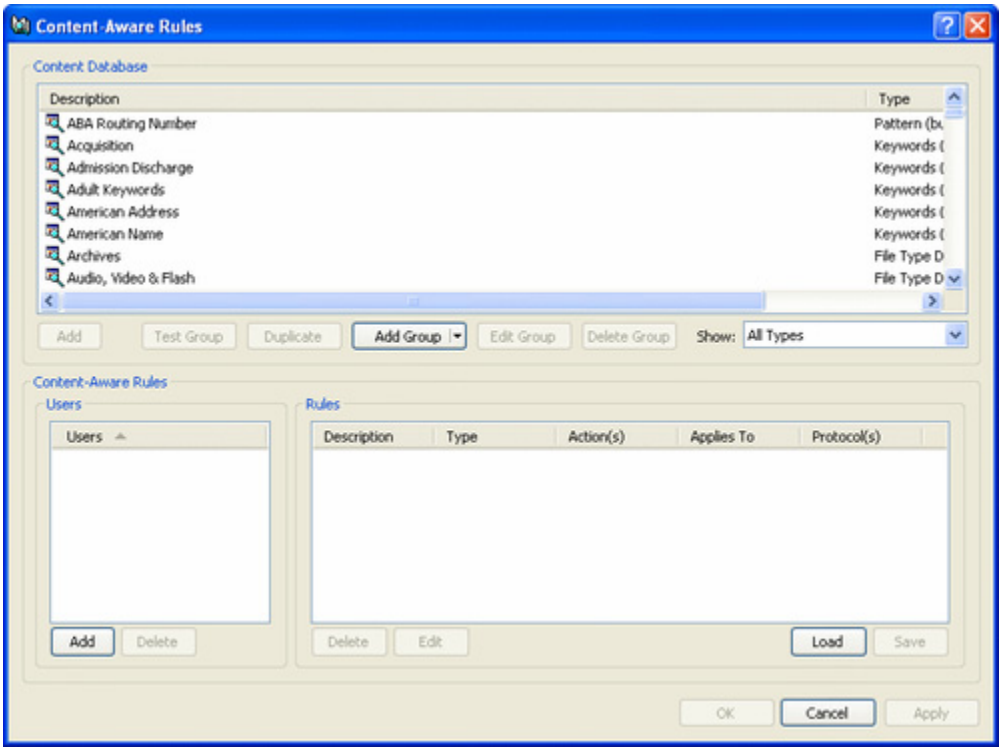
Per definire una regola basata sul contenuto (Content-Aware Rule)

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere Computer Configuration, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la regola, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules.

   Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

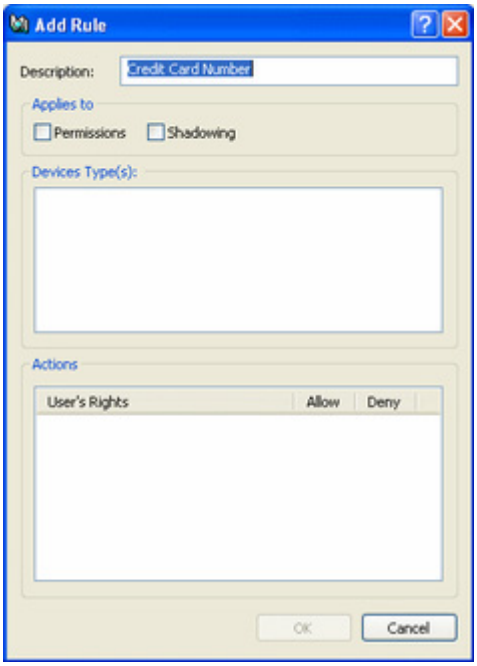
6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare gli utenti o i gruppi per cui si desidera definire la regola.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

7. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **Add**.

   Nota: è possibile specificare un solo gruppo di contenuto per ogni regola basata sul contenuto.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, nella casella **Description**, digitare il nome della regola basata sul contenuto.

   Per impostazione predefinita, quest'ultima ha lo stesso nome del gruppo di contenuto specificato, ma è possibile specificare un altro nome.

9. Sotto **Applies to**, specificare il tipo di operazione associata con la regola. Le opzioni disponibili sono:
   - **Permissions**: specifica che la regola verrà applicata alle operazioni di controllo dell'accesso.
   - **Shadowing**: specifica che la regola verrà applicata alle operazioni di copia shadow.
   - **Permissions**, **Shadowing**: specifica che la regola verrà applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.

10. Sotto **Device Type(s)**, selezionare i tipi di periferica appropriati a cui si desidera applicare la regola.

    Le regole basate sul contenuto possono essere applicate ai tipi di periferica DVD/CD-ROM, Floppy, iPhone, Palm, Removable e Windows Mobile.

    Se vengono selezionati più tipi di periferica con diversi diritti di accesso, nella finestra di dialogo sotto Action(s) vengono visualizzati solo i diritti di accesso comuni per tutti i tipi di periferica selezionati.

11. Sotto **Action(s)**, specificare quali azioni degli utenti sono autorizzate o non autorizzate per i file e quali azioni degli utenti vanno inserite nel registro shadowing.

    È possibile selezionare una qualsiasi delle seguenti opzioni: Read (lettura), Write (scrittura) e Read and Write (lettura e scrittura).

Se la regola viene applicata alle operazioni di copia shadow o sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow, l'opzione Read non è disponibile. Per informazioni dettagliate sui diritti degli utenti che possono essere specificati nelle regole basate sui contenuti, consultare le sezioni "Regole basate sul contenuto per le operazioni di controllo dell'accesso" e "Regole basate sul contenuto per le operazioni di copia shadow".

12. Fare clic su **OK**.

    La regola creata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules.

13. Fare clic su **OK** o su **Apply** per applicare la regola.

    Gli utenti o i gruppi per cui è stata applicata la regola basata sul contenuto vengono visualizzati sotto Content-Aware Rules nella struttura della console. Se nella struttura della console viene selezionato un utente o un gruppo per cui è stata applicata una regola basata sul contenuto, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:

    - **Description** Il nome della regola. Per impostazione predefinita, la regola ha lo stesso nome del gruppo di contenuto specificato.
    - **Type** Il tipo di analisi del contenuto. Valori possibili: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties** e **Complex**. **File Type Detection** indica che il riconoscimento e l'identificazione dei file si basa sulle loro firme caratteristiche. **Keywords** indica che il riconoscimento e l'identificazione dei file/dati si basa sulle parole chiave o frasi specificate. **Pattern** indica che il riconoscimento e l'identificazione dei file/dati si basa sui motivi di testo specificati descritti dalle espressioni comuni Perl. **Document Properties** indica che il riconoscimento e l'identificazione dei file si basa sulle loro proprietà. **Complex** indica che il riconoscimento e l'identificazione dei file/dati si basa sul contenuto specificato descritto da un'espressione booleana.
    - **Action(s)** Mostra quali azioni degli utenti sono autorizzate o non autorizzate per i file e quali azioni degli utenti vanno inserite nel registro shadowing.
    - **Applies To** Valori possibili: **Permissions**, **Shadowing**, e **Permissions, Shadowing**. **Permissions** indica che la regola viene applicata alle operazioni di controllo dell'accesso. **Shadowing** indica che la regola viene applicata alle operazioni di copia shadow. **Permissions, Shadowing** indica che la regola viene applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.
    - **Device Type(s)** Il tipo (o i tipi) di dispositivo per cui viene applicata la regola.
    - **Profile** Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

      È possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire le Content-Aware Rules offline, consultare la sezione "Gestione delle regole basate sul contenuto offline per le periferiche".

Modifica delle regole basate sul contenuto

È possibile modificare le proprietà delle Content-Aware Rules (regole basate sul contenuto) come Description, Applies To, Device Type(s) e Actions (Descrizione, Si applica a, Tipi di periferica e Azioni).

Come modificare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, scegliere **Manage**, quindi attenersi alla procedura seguente:

   a) Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

   b) Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.
   - OPPURE -
   Fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Edit** nel menu di scelta rapida.

   - OPPURE -

   Sotto **Devices**, espandere **Content-Aware Rules**, quindi attenersi alla procedura seguente:

   a) Sotto **Content-Aware Rules**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto applicati agli stessi nel riquadro dei dettagli.

   b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.
   - OPPURE -
   Nel riquadro dei dettagli, fare doppio clic sulla regola che si desidera modificare.

   Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare le proprietà della regola a seconda delle proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole basate sul contenuto

Per riutilizzare le regole basate sul contenuto (Content-Aware Rules) esistenti, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Come copiare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

5. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. Se si usa la combinazione di tasti CTRL+X, la regola viene tagliata solo dopo essere stata incollata.

   Per eseguire un'operazione di trascinamento, selezionare la regola e spostarla verso l'utente o il gruppo a cui si desidera applicare la regola copiata.

6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi a cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules.

8. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare gli utenti o i gruppi a cui applicare la regola copiata.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

9. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, fare clic con il pulsante destro del mouse sul riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules.

10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione delle regole basate sul contenuto

È possibile esportare tutte le Content-Aware Rules (regole basate sul contenuto) correnti in un file .cwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare le regole basate sul contenuto

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Save**.
     - OPPURE -

- Selezionare **Content-Aware Rules**, quindi fare clic su **Save** sulla barra degli strumenti.
  - OPPURE -
- Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo a cui viene applicata la regola, quindi scegliere **Save**.
  - OPPURE -
- Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Save**.
  - OPPURE -
- Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Save** sulla barra degli strumenti.
  - OPPURE -
- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic su **Save**.

Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .cwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   Le regole esportate vengono salvate in un file con estensione .cwl.

Come importare le regole basate sul contenuto

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Load**.
     - OPPURE -

- Selezionare **Content-Aware Rules**, quindi fare clic su **Load** sulla barra degli strumenti.

  - OPPURE -

- Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo a cui viene applicata la regola, quindi scegliere **Load**.

  - OPPURE -

- Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Load**.

  - OPPURE -

- Espandere Content-Aware Rules, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Load** sulla barra degli strumenti.

  - OPPURE -

- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic su **Load**.

Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   È possibile importare un solo file .cwl alla volta.

Rimozione della definizione delle regole basate sul contenuto

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che le regole basate sul contenuto vengano applicate a un gruppo specifico di computer client. Per farlo, occorre riportare le regole basate sui contenuti precedentemente definite al loro stato non configurato. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Come rimuovere la definizione delle regole basate sul contenuto

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
   c) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.

b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Undefine**.

Eliminazione delle regole basate sul contenuto

Quando alcune Content-Aware Rules (regole basate sul contenuto) non sono più necessarie, possono essere eliminate.

Come eliminare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo a cui viene applicata la regola, quindi scegliere **Delete user**.
     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.

     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.
     È possibile selezionare più regole da eliminare tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sulle regole.

Regole basate sul contenuto per i protocolli (Regular Profile)

Le regole basate sul contenuto (Content-Aware Rules) migliorano la funzionalità del controllo dell'accesso ai protocolli di DeviceLock aggiungendo una protezione completa a livello di contenuto dei dati aziendali contenenti informazioni riservate. Le regole basate sul contenuto consentono di eseguire l'ispezione automatica dei dati/file trasmessi sulla rete, il rilevamento del contenuto riservato e l'applicazione dei criteri normativi per garantire la protezione.

Le regole basate sul contenuto consentono di concedere o negare in maniera selettiva l'accesso a determinati contenuti trasmessi sulla rete, indipendentemente dalle autorizzazioni prestabilite a livello di protocollo. Le regole basate sul contenuto, inoltre, possono essere utilizzate per autorizzare o negare la copia shadow di determinati contenuti. Le regole basate sul contenuto sono flessibili e possono essere definite a livello di utente o di gruppo.

È possibile configurare le regole basate sul contenuto per le operazioni di controllo dell'accesso, per le operazioni di copia shadow, o per entrambe.

Seguono alcuni esempi di utilizzo delle regole basate sul contenuto (Content-Aware Rules).

- **Esempio 1 - Utilizzo delle regole basate sul contenuto per le operazioni di controllo dell'accesso**. È possibile negare a determinati utenti o gruppi il caricamento di file contenenti numero di carta di credito, numeri telefonici e indirizzi su un sito Web FTP.
- **Esempio 2 - Utilizzo delle regole basate sul contenuto per le operazioni di copia shadow**. È possibile specificare l'esecuzione della copia shadow per le conversazioni di messaggistica immediata contenenti numero di carta di credito e indirizzi e-mail, ai fini delle verifiche di sicurezza e delle indagini sugli incidenti.

Nota: è possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Le regole basate sul contenuto online (Regular Profile) si applicano ai computer client che operano online. Le regole basate sul contenuto offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire le regole basate sul contenuto offline per i protocolli, consultare la sezione "Gestione delle regole basate sul contenuto offline per i protocolli".

Regole basate sul contenuto per le operazioni di controllo dell'accesso

Le regole basate sul contenuto (Content-Aware Rules) consentono di:

- Autorizzare l'accesso a determinati contenuti quando l'accesso è negato a livello di protocollo.
- Negare l'accesso a determinati contenuti quando l'accesso è consentito a livello di protocollo.

Le regole basate sul contenuto (Content-Aware Rules) hanno la precedenza su tutte le regole definite nella lista bianca dei protocolli.

La seguente tabella fornisce un riepilogo dei diritti di accesso che possono essere specificati per ciascun protocollo nelle regole basate sul contenuto.

PROTOCOLLO	DIRITTI DI ACCESSO	DESCRIZIONE
FTP	Generic: Outgoing Files	Determina se l'utente può caricare file con determinati contenuti su un server FTP.
	SSL: Outgoing Files	Determina se l'utente può caricare file con determinati contenuti su un server FTP utilizzando FTPS.
HTTP	Generic: POST Requests	Determina se l'utente può inoltrare dati di moduli Web con determinati contenuti su un server Web utilizzando HTTP.
	Generic: Outgoing Files	Determina se l'utente può caricare file con determinati contenuti su un server Web utilizzando HTTP.
	SSL: POST Requests	Determina se l'utente può inoltrare dati di moduli Web con determinati contenuti su un server Web utilizzando HTTPS.
	SSL: Outgoing Files	Determina se l'utente può caricare file con determinati contenuti su un server Web utilizzando HTTPS.
ICQ/AOL Messenger, IRC, Jabber	Generic: Outgoing Messages	Determina se l'utente può inviare messaggi immediati con determinati contenuti.
	SSL: Outgoing Messages	Determina se l'utente può inviare messaggi immediati con determinati contenuti utilizzando SSL.
Mail.ru Agent, Windows Messenger, Yahoo Messenger	Generic: Outgoing Messages	Determina se l'utente può inviare messaggi immediati con determinati contenuti.
SMTP, Web Mail	Generic: Outgoing Messages	Determina se l'utente può inviare messaggi e-mail con determinati contenuti.
	Generic: Outgoing Files	Determina se l'utente può inviare allegati e-mail con determinati contenuti.
	SSL: Outgoing Messages	Determina se l'utente può inviare messaggi e-mail con determinati contenuti utilizzando SSL.

PROTOCOLLO	DIRITTI DI ACCESSO	DESCRIZIONE
	SSL: Outgoing Files	Determina se l'utente può inviare allegati e-mail con determinati contenuti utilizzando SSL.
Social Networks	Generic: Outgoing Messages	Determina se l'utente può inviare messaggi, commenti e post con determinati contenuti.
	Generic: Outgoing Files	Determina se l'utente può inviare file multimediali o di altro tipo con determinati contenuti sul sito di una rete sociale.

Nota: se è impostata l'autorizzazione No Access per un protocollo ed è presente una regola basata sul contenuto (Content-Aware Rule) che consente l'accesso al contenuto specificato per lo stesso protocollo, il diritto di accesso Send/Receive Data viene concesso automaticamente agli utenti per questo protocollo. Per ulteriori informazioni su questo diritto di accesso, consultare la sezione "Gestione delle autorizzazione per i protocolli".

Durante l'utilizzo delle regole basate sul contenuto (Content-Aware Rules), considerare quanto segue:

- ***Se le regole basate sul contenuto sono state definite sia per le periferiche sia per i protocolli, tutti i controlli dell'accesso vengono eseguiti in un thread***.
- ***Le regole basate sul contenuto con impostazione Deny (Nega) hanno la priorità su quelle con impostazione Allow (Autorizza) se si applicano agli stessi utenti o agli stessi gruppi***.
- ***La verifica del contenuto dei file è un'operazione che può richiedere molto tempo. È possibile definire un messaggio di verifica del contenuto da mostrare agli utenti durante l'esecuzione dell'ispezione del contenuto. Per informazioni dettagliate su questo messaggio, consultare la sezione "Content verification message" (Messaggio di verifica del contenuto) in "Service Options"***.
- ***Se gli utenti tentano di utilizzare i protocolli per cui non dispongono dell'accesso, viene visualizzato un messaggio di blocco dei protocolli, se l'opzione Protocols blocked message è stata selezionata in Service Options. Per informazioni dettagliate su questo messaggio, consultare la sezione "Protocols blocked message" (Messaggio di blocco dei protocolli) in "Service Options"***.

Regole basate sul contenuto per le operazioni di copia shadow

Prima di poter utilizzare le regole basate sul contenuto (Content-Aware Rules) per le operazioni di copia shadow, è necessario attivare lo shadowing in **Auditing and Shadowing** a livello di tipo protocollo. Le regole basate sul contenuto che si applicano alle operazioni di copia shadow filtrano le copie shadow dei dati e dei file trasmessi dall'utente.

La seguente tabella fornisce un riepilogo dei diritti di shadowing che possono essere specificati per ciascun protocollo nelle regole basate sul contenuto.

PROTOCOLLO	DIRITTI DI COPIA SHADOW	DESCRIZIONE
FTP	Generic: Incoming Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti scaricati da un server FTP.
	Generic: Outgoing Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti caricati su un server FTP.
	SSL: Incoming Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti scaricati da un server FTP utilizzando FTPS.
	SSL: Outgoing Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti caricati su un server FTP utilizzando FTPS.
HTTP	Generic: Incoming Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti scaricati da un server Web.
	Generic: POST Requests	Determina se eseguire o meno la copia shadow dei dati dei moduli Web con determinati contenuti inoltrati su un server Web.
	Generic: Outgoing Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti caricati su un server Web.
	SSL: Incoming Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti scaricati da un server Web utilizzando HTTPS.
	SSL: POST Requests	Determina se eseguire o meno la copia shadow dei dati dei moduli Web con determinati contenuti inoltrati su un server Web utilizzando HTTPS.
	SSL: Outgoing Files	Determina se eseguire o meno la copia shadow dei file con determinati contenuti caricati su un server Web utilizzando HTTPS.
ICQ/AOL Messenger, IRC, Jabber	Generic: Incoming Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti ricevuti dall'utente.
	Generic: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti inviati dall'utente.
	SSL: Incoming Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti ricevuti dall'utente utilizzando SSL.

PROTOCOLLO	DIRITTI DI COPIA SHADOW	DESCRIZIONE
	SSL: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti inviati dall'utente utilizzando SSL.
Mail.ru Agent, Windows Messenger, Yahoo Messenger	Generic: Incoming Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti ricevuti dall'utente.
	Generic: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi immediati con determinati contenuti inviati dall'utente.
SMTP, Web Mail	Generic: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi e-mail con determinati contenuti inviati dall'utente.
	Generic: Outgoing Files	Determina se eseguire o meno la copia shadow degli allegati e-mail con determinati contenuti inviati dall'utente.
	SSL: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi e-mail con determinati contenuti inviati dall'utente utilizzando SSL.
	SSL: Outgoing Files	Determina se eseguire o meno la copia shadow degli allegati e-mail con determinati contenuti inviati dall'utente utilizzando SSL.
Social Networks	Generic: Outgoing Messages	Determina se eseguire o meno la copia shadow dei messaggi, dei commenti e dei post con determinati contenuti inviati dall'utente.
	Generic: Outgoing Files	Determina se eseguire o meno la copia shadow dei file multimediali o di altro tipo con determinati contenuti caricati sul sito di una rete sociale.

Configurazione delle impostazioni di rilevamento del contenuto

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto, che consentono di definire centralmente i tipi di contenuto per cui verificare l'accesso. I gruppi di contenuto specificano i criteri di filtraggio del contenuto che verranno utilizzati per selezionare i dati a cui applicare le regole.

Tutti i gruppi di contenuto sono memorizzati nel database dei contenuti. Per le periferiche e i protocolli viene utilizzato lo stesso database dei contenuti. Il database dei contenuti, che fa parte dei criteri di DeviceLock Service, viene salvato in un file XML contenente le impostazioni del servizio. Questo file può essere creato utilizzando DeviceLock Management Console, DeviceLock Service Settings Editor e DeviceLock Group Policy Manager.

Sono disponibili diversi tipi di gruppi di contenuto: File Type Detection (Rilevamento tipo file), Keywords (Parole chiave), Pattern (Motivi), Document Properties (Proprietà documenti) e Complex (Complessi). La sezione sottostante descrive i gruppi e spiega come utilizzarli.

Gruppi di contenuto File Type Detection (Rilevamento tipo file)

I gruppi File Type Detection vengono utilizzati per controllare l'accesso ai file in base ai tipi di file. Questi gruppi contengono le definizioni del tipo di file inclusi nei gruppi. Una definizione del tipo di file è composta da due proprietà: l'estensione del file (ad esempio DOC) e la descrizione (ad esempio documento di Microsoft Word). Quando viene applicata una regola basata su un gruppo File Type Detection, la regola viene applicata a tutti i tipi di file inclusi nel gruppo.

DeviceLock include 34 gruppi File Type Detection predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
Archives	MS Outlook & Outlook Express
Audio, Video & Flash	MS PowerPoint
BlackBerry	MS Project
Common Object File Format (COFF)	MS Publisher
Database	MS Visio
Executable	MS Windows Installer
Fax Documents	MS Windows Memory Dump
FileMaker Pro	MS Word
Fonts	MS Works
Help Files	OpenOffice, StarOffice, OpenDocument, etc.
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
Lotus SmartSuite	QuickBooks, Quicken, TurboTax & etc.
MS Access	Rich Text Format
MS Excel	Security Certificates
MS InfoPath	Text, HTML & XML
MS Money	Virtual Machines
MS OneNote	WordPerfect Office

Nota: le regole basate sul contenuto supportano i formati Word To Go, Sheet To Go e Slideshow To Go per i dispositivi Palm. Il formato Word To Go è incluso nei gruppi di contenuto incorporati MS Word e Rich Text Format, il formato Sheet To Go è incluso nel gruppo di contenuto incorporato MS Excel e il formato Slideshow To Go è incluso nel gruppo di contenuto incorporato MS PowerPoint.

I file Microsoft Word, RTF (Rich Text Format), Excel e PowerPoint possono essere trasferiti su un dispositivo Palm utilizzando l'applicazione Documents To Go. L'applicazione Documents To Go converte questi file in formati speciali: i file Word e RTF in formato Word To Go, i file Excel in formato Sheet To Go e i file PowerPoint in formato Slideshow To Go. I file convertiti vengono scaricati automaticamente sul dispositivo Palm quando l'utente esegue la sincronizzazione.

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare le definizioni del tipo di file incluse nei gruppi File Type Detection incorporati, ma non modificarle né eliminarle. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione "Visualizzazione dei gruppi di contenuto incorporati".

Creazione di gruppi di contenuto File Type Detection personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto File Type Detection personalizzati consentono di specificare qualsiasi tipo di file da includere nello stesso gruppo, in base alle esigenze specifiche di ciascun utente.

Si supponga di voler garantire a determinati utenti l'accesso ai documenti Word, Excel e PDF e ai file di grafica. Per farlo, occorre innanzitutto creare un nuovo gruppo di contenuto che rappresenti questi tipi di documenti. In seguito, si può definire una regola basata su questo gruppo di contenuto personalizzato.

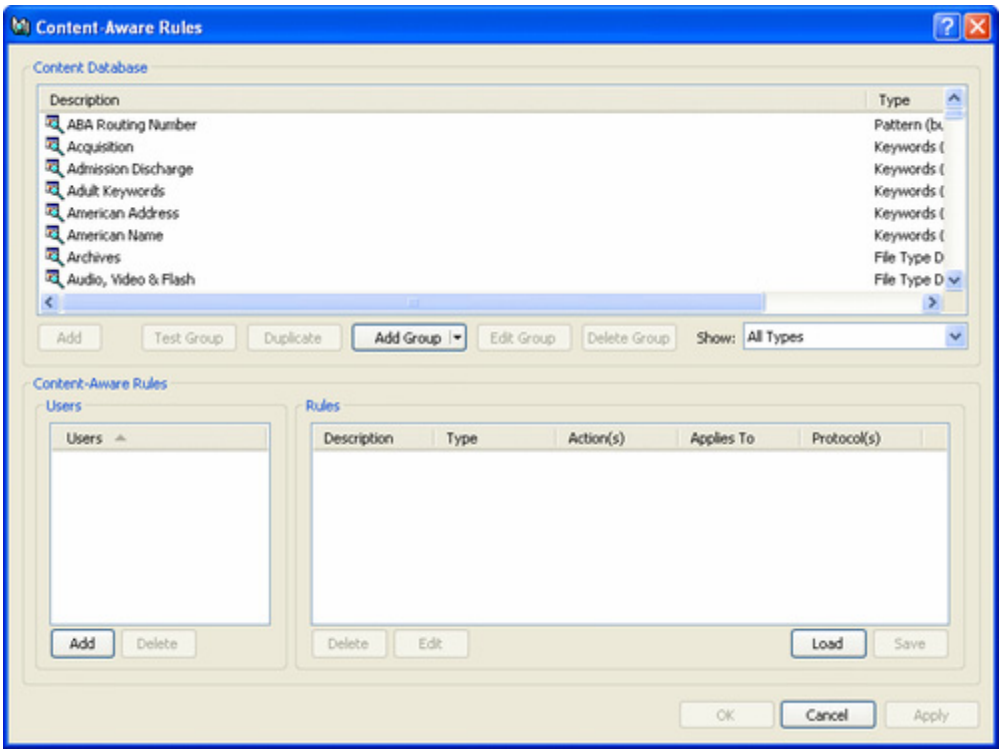
Per creare un gruppo File Type Detection personalizzato

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

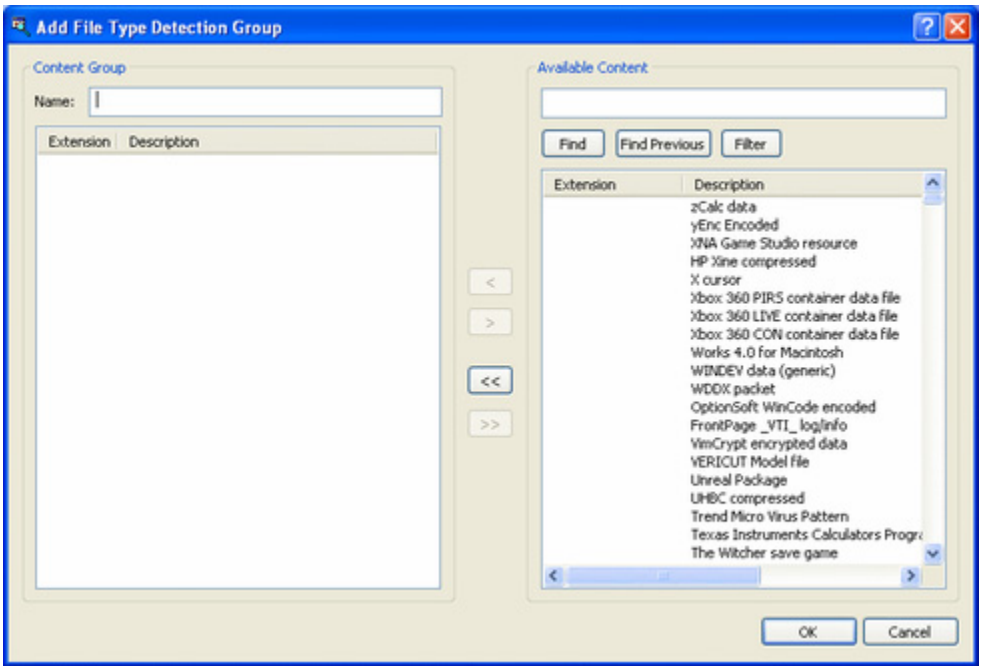
   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **File Type Detection**.

   Viene visualizzata la finestra di dialogo Add File Type Detection Group.



5. Nel riquadro sinistro della finestra di dialogo **Add File Type Detection Group**, sotto **Content group**, digitare il nome del nuovo gruppo di contenuto nella casella **Name**.

   Nota: un nuovo gruppo di contenuto non può avere lo stesso nome di un gruppo di contenuto esistente.

6. Nel riquadro destro della finestra di dialogo **Add File Type Detection Group**, sotto **Available Content**, selezionare il tipo di file da aggiungere al nuovo gruppo di contenuto, quindi fare clic sul pulsante della freccia singola a sinistra <.

   È possibile selezionare più tipi di file tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui tipi di file.

   Per rimuovere singoli tipi di file dal gruppo di contenuto, utilizzare il pulsante della freccia singola a destra >. Per aggiungere/rimuovere simultaneamente tutti i tipi di file disponibili al/dal gruppo di contenuto, utilizzare il pulsante della doppia freccia a sinistra << o della doppia freccia a destra >>.

   Nota: è possibile eseguire ricerche nel database di contenuto disponibile per tipi di file specifici tramite l'estensione o la descrizione. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?) per cercare un gruppo specifico di tipi di file. Per trovare un tipo di file o un gruppo di tipi di file specifico, sotto **Available Content** digitare un'estensione o una descrizione (con o senza caratteri jolly) nella stringa di ricerca, quindi fare clic su **Find**. Per applicare un filtro ai tipi di file, fare clic su **Filter**. Per rimuovere il filtro, applicarlo a una stringa vuota.

   Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità.

7. Fare clic su **OK** per chiudere la finestra di dialogo **Add File Type Detection Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Keywords (Parole chiave)

I gruppi Keywords vengono utilizzati per controllare l'accesso ai dati/file in base a determinate parole chiave o frasi.

DeviceLock include 157 gruppi Keywords predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
Accounting Documentation Terms	Production Charges
Accounting Documentation Types	Profanity
Acquisition	Profiles
Active substance	Profit Loss

GRUPPI DI CONTENUTO PREDEFINITI

Admission Discharge	Project Names
Adult Keywords	Project Release Dates
American Address	Property
American Name	Racism Keywords
Bank ABA	Resume
Bank ACNT	Russian: Account Statement
Bank STMT	Russian: Accounting Documentation
Board Meeting	Russian: Accounting Documentation Terms
Breach of Obligation	Russian: Accounting Documentation Types
Breach of Standards	Russian: Bank Account
Breach of the Law	Russian: Bank Operations
Business Documentation	Russian: Banking Operations Participants
Business Documentation Terms	Russian: Breach of Commitment
Business Documentation Types	Russian: Breach of Law
Business Rivals	Russian: Business Documentation
Business Trips & Meetings	Russian: Business Documentation Terms
C# Source Code	Russian: Business Documentation Types
C/C++ Source Code	Russian: Business Partners
Cellular Operator Call Log	Russian: Business Trips & Meetings
COBOL Source Code	Russian: Company Development Plan
Common Disease	Russian: Compensation and Benefits
Common Medical Terms	Russian: Confidential Information
Company Development	Russian: Corporate Capital
Compensation and Benefits	Russian: Corporate Property
Compliance Report	Russian: Expenses
Confidential	Russian: Failures
Confidential Partners Information	Russian: Financial Information
Credit Report	Russian: Financial Report
Credits	Russian: Financial Terms
Discontent	Russian: Firing
Discrediting Information	Russian: Innovations
Driver’s License	Russian: Insurance
Employer Identification Number	Russian: Internal Payments
Ethnicity	Russian: Investors and Investments
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medicinal Active Substances
FITS Date & Time	Russian: Medicinal Drugs
FITS File Checksum	Russian: Noncompliant
FITS File Descriptors	Russian: Passwords and Access Codes
FITS Hierarchical file grouping	Russian: Physical Security
FITS Instrumentorum	Russian: Prices
FITS Non-standard	Russian: Project Documentation
FITS Observations	Russian: Project Names
FITS Standard	Russian: Project Versions
Gambling	Russian: Projects Release Date
Grades	Russian: Technology
HCFA (CMS) 1500 Form	Russian: User Names
HIPAA - Diseases	Russian: Working Conditions
HIPAA HCPCS	Sales Forecast
HIPAA ICD9	Sarbanes-Oxley Sensitive
HIPAA NDC Classes	Security
HIPAA NDC Dosages	Security Agencies
HIPAA NDC Listing	Sensitive Disease

GRUPPI DI CONTENUTO PREDEFINITI	
HIPAA NDC Routes	Sexual Language
Illegal Drugs	Social Security
Innovations	SPAM
Internet Slang Abbreviations	Sports
Investments	Staff Training
Java Source Code	Substance Abuse
Market Development	Suspicious Activity Report
Medical Diagnosis	Technology
Medical Record Numbers	UBO4 Form
MEMO	US Birth Date
Network Security	US Birth Place
Partner Names	US Expiry Date
Password	User Name
Payments	VB Source Code
PCI GLBA	Violence
Perl Source Code	Weapon Keywords
Price List	Wire Transfer
Prices	Working Conditions
Pro Earnings	

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare le parole chiave incluse nei gruppi Keywords incorporati, ma non modificarle né eliminarle. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione "Visualizzazione dei gruppi di contenuto incorporati".

Creazione di gruppi Keywords (Parole chiave) personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto Keywords personalizzati consentono di specificare qualsiasi tipo di parola chiave da includere nello stesso gruppo, in base alle esigenze specifiche di ciascun utente.

Per creare un gruppo Keywords personalizzato

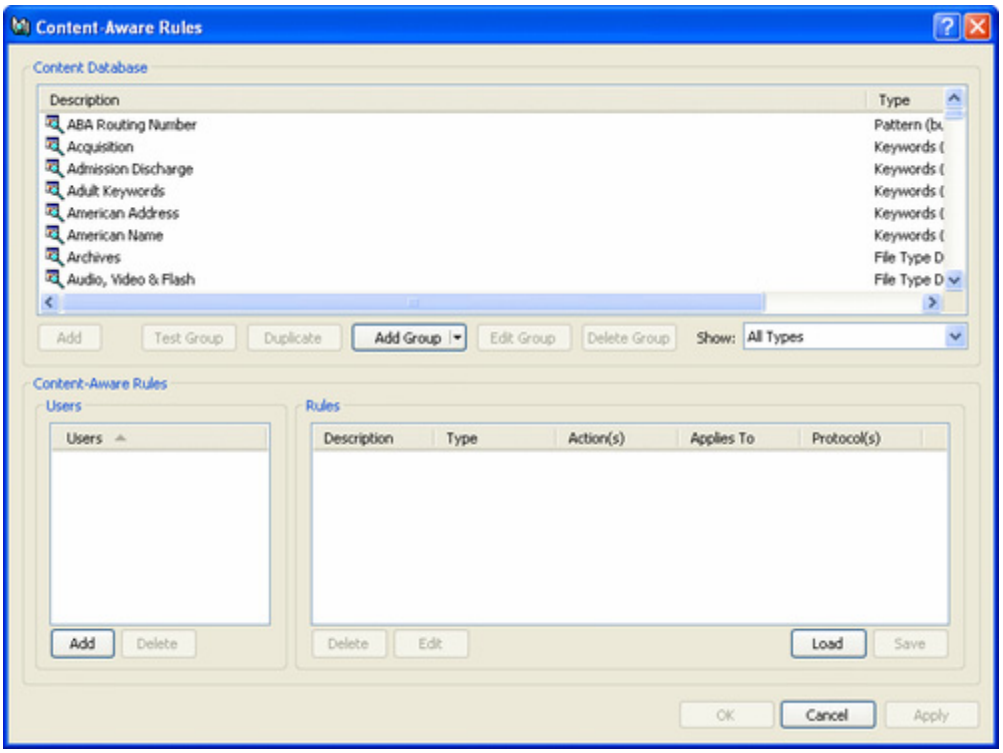
1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.

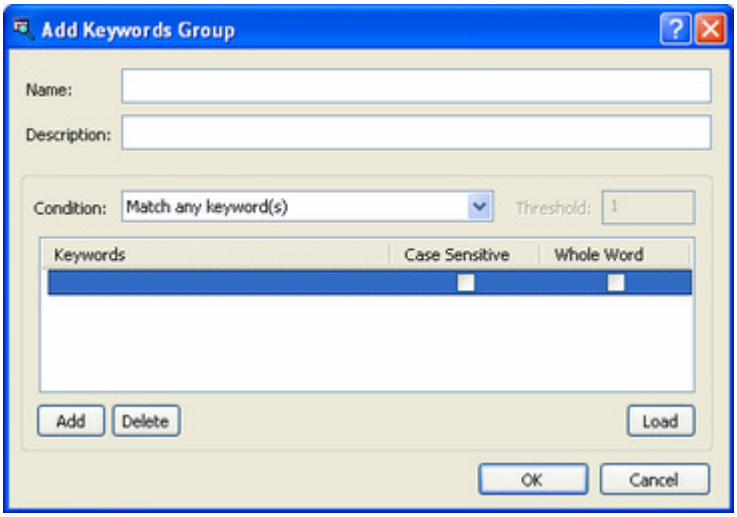
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Keywords**.

   Viene visualizzata la finestra di dialogo Add Keywords Group.



5. Nella finestra di dialogo **Add Keywords Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Condition:	Specificare le condizioni delle regole di attivazione associate a questo gruppo di contenuto. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Condition**: • **Match any keyword(s)**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che una qualsiasi delle parole chiave specificate viene rilevata tra i dati di testo. • **Match all keyword(s)**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che tutte le parole chiave specificate vengono rilevate tra i dati di testo. • **Only when combined score exceeds (or equal to) threshold**: indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero totale (la somma) delle occorrenze di tutte le parole chiave rilevate tra i dati di testo raggiunge o supera la soglia delle occorrenze di parole chiave.
Threshold	Specificare il numero di occorrenze delle parole chiave della soglia. Il numero deve essere compreso tra 0 e 65535. Se è stata specificata l'opzione **Only when combined score exceeds (or equal to) threshold**, questa proprietà richiede un valore.
Keywords	Specificare le parole e le frasi che devono verificarsi tra i dati di testo. Fare doppio clic sotto **Keywords** per immettere una parola chiave o una frase.
Case Sensitive	Determinare il tipo di distinzione tra maiuscole e minuscole delle parole chiave. Selezionare la casella di controllo **Case Sensitive** per attivare la distinzione tra maiuscole e minuscole delle parole chiave (ad esempio, le parole "test" e "Test" verranno trattate come due parole chiave distinte). Deselezionare la casella di controllo **Case Sensitive** per disattivare la distinzione tra maiuscole e minuscole delle parole chiave (ad esempio, le parole "test" e "Test" verranno considerate come un'unica parola chiave).
Whole Word	Specificare le opzioni di corrispondenza con le parole chiave. Selezionare la casella di controllo **Whole Word** per specificare l'opzione di corrispondenza esatta (consente di trovare una corrispondenza esatta con la parola chiave). Deselezionare la casella di controllo **Whole Word** per specificare l'opzione di corrispondenza più estesa (consente di trovare tutte le varianti grammaticali della parola chiave).
Weight	Specificare il grado di importanza di ciascuna parola chiave o frase. Questo valore viene utilizzato per contare il numero di occorrenze delle parole chiave specificate tra i dati di testo. Se è stata specificata l'opzione **Only when combined score exceeds (or equal to) threshold**, questa proprietà richiede un valore.

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	Valori possibili: **Heavy**, **Above Normal**, **Normal** (valore predefinito), **Below Normal**, **Light**. Interpretazione dei valori: **Heavy** indica che ciascuna ocorrenza di parola chiave viene contata come tre occorrenze. Si tratta del valore più elevato. **Above normal** indica che ciascuna ocorrenza di parola chiave viene contata come due occorrenze. **Normal** indica che ciascuna ocorrenza di parola chiave viene contata come un'occorrenza. **Below normal** indica che due occorrenze di parola chiave vengono contate come un'occorrenza. **Light** indica che tre occorrenze di parola chiave vengono contate come un'occorrenza. Si tratta del valore più basso.
Add	Specificare le parole chiave e le frasi. Fare clic su **Add** per immettere una parola chiave o una frase.
Delete	Eliminare una parola chiave. Per farlo, selezionare la parola chiave che si desidera eliminare e fare clic su **Delete**. È possibile selezionare più parole chiave tenendo premuto il tasto MAIUSC o CTRL e facendo clic sulle parole chiave.
Load	Importare un elenco di parole chiave da un file di testo delimitato da tabulazione.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Keywords Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Pattern (Motivi)

I gruppi Pattern consentono di controllare l'accesso ai dati di testo utilizzando motivi di testo descritti dalle espressioni comuni Perl. I motivi rappresentano uno strumento efficace e flessibile per eseguire il rilevamento automatico di contenuti potenzialmente riservati (ad esempio numeri di carta di credito e di codice fiscale, indirizzi e-mail e numeri di telefono) all'interno dei dati di testo.

Per ulteriori informazioni sulla creazione e l'utilizzo delle espressioni comuni Perl, consultare le sezioni Guida introduttiva alle espressioni comuni Perl e Guida alle espressioni comuni Perl.

DeviceLock include 45 gruppi Pattern predefiniti (incorporati) che possono essere usati per impostare la configurazione desiderata delle operazioni di autorizzazione e/o di copia

shadow. È possibile utilizzare i gruppi di contenuto incorporati, creare copie modificabili di questi ultimi (duplicati) o generare gruppi personalizzati in base alle esigenze della propria organizzazione.

La seguente tabella contiene un elenco di questi gruppi di contenuto predefiniti:

GRUPPI DI CONTENUTO PREDEFINITI	
ABA Routing Number BIC (ISO 9362) Canadian Social Insurance Number Credit Card Number Email Address European VAT Number GPS Data (RMC String) IBAN International Telephone Number IP Address ISO Date MAC Address Microsoft Windows Product Key Russian: Address Russian: Auto Insurance Number Russian: Bank Account Number Russian: BIC Russian: Car Numbers Russian: Classification of Economic Activities Russian: Classification of Enterprises and Organizations Russian: Driver's License Number Russian: Health Insurance Number Russian: International Passport	Russian: Main State Registration Number Russian: Motorcycle Numbers Russian: Passport Russian: Pension Insurance Number Russian: Post Code Russian: Taxpayer Identification Number Russian: Telephone Number Russian: Trailer Numbers Russian: Vehicle Registration Document SQL Queries TCP/UDP Port Number Time (12/24h) UK National Insurance Number UK Phone Number UK Post Code UK Tax Code Uniform Resource Locator (URL) US Date US Phone Number US Social Security Number US Zip Code VIN

Utilizzando i gruppi di contenuto incorporati, è possibile creare e applicare rapidamente delle regole senza dover definire gruppi di contenuto propri.

Nota: è possibile visualizzare i motivi di espressioni comuni nei gruppi Pattern incorporati, ma non modificarli né eliminarli. Per informazione su come visualizzare i gruppi di contenuto incorporati, consultare la sezione "Visualizzazione dei gruppi di contenuto incorporati".

Creazione di gruppi Pattern (Motivi) personalizzati

Se i gruppi di contenuto predefiniti di DeviceLock non soddisfano i requisiti dell'utente, questi può definire le Content-Aware Rules (regole basate sul contenuto) tramite gruppi di contenuti personalizzati. I gruppi di contenuto Pattern personalizzati consentono di specificare qualsiasi motivo da utilizzare per identificare le informazioni riservate nei dati di testo.

Per creare un gruppo Pattern personalizzato

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

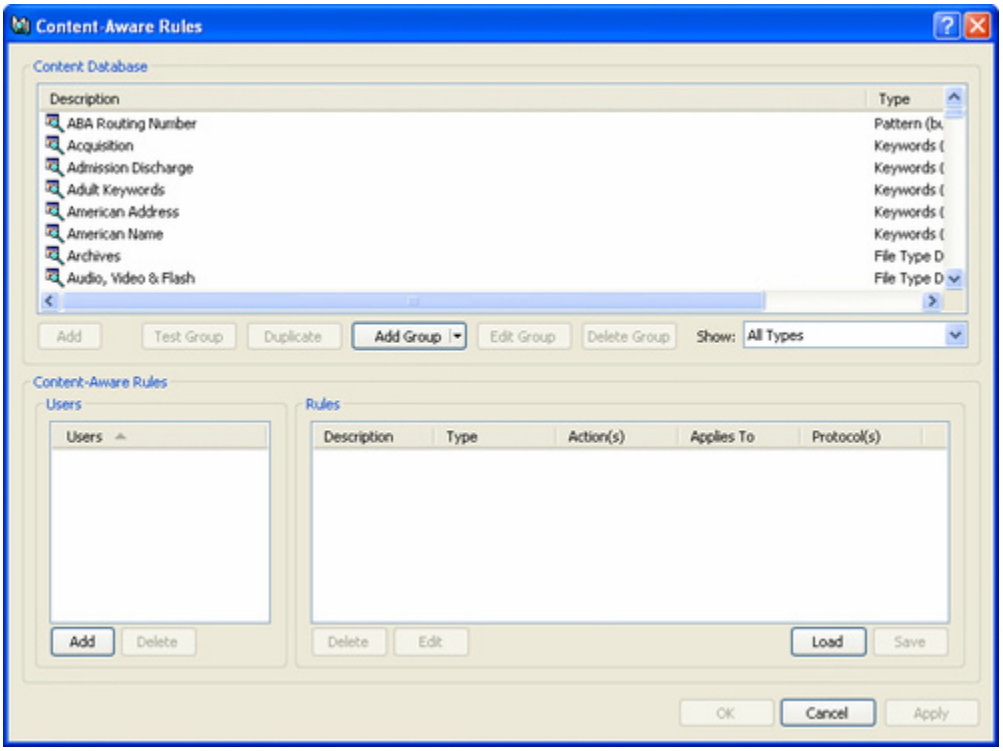
a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

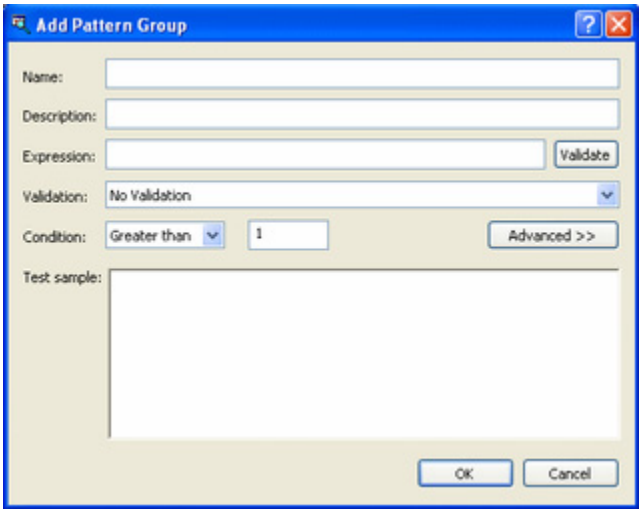
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Pattern**.

   Viene visualizzata la finestra di dialogo Add Pattern Group.



5. Nella finestra di dialogo **Add Pattern Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Expression	Specificare un motivo creando un'espressione comune. Per informazioni sulla creazione delle espressioni comuni Perl, consultare le sezioni Guida introduttiva alle espressioni comuni Perl e Guida alle espressioni comuni Perl.
Validate	Verificare la sintassi dell'espressione comune.
Validation	Eseguire la convalida delle corrispondenze potenziali restituite dall'espressione comune. Sono disponibili le seguenti opzioni: **No validation** (opzione predefinita), **ABA Routing Number**, **Canadian Social Insurance Number**, **Credit Card Number (All)**, **Credit Card Number (American Express)**, **Credit Card Number (Diners Club)**, **Credit Card Number (Diners Club En Route)**, **Credit Card Number (Discover)**, **Credit Card Number (JCB)**, **Credit Card Number (Laser)**, **Credit Card Number (Maestro)**, **Credit Card Number (Master Card)**, **Credit Card Number (Solo)**, **Credit Card Number (Switch)**, **Credit Card Number (Visa)**, **Credit Card Number (Visa Electron)**, **Date, Date (ISO)**, **Email Address**, **European VAT Number**, **IBAN**, **IP Address**, **LUHN Checksum**, **Russian Bank Account Number**, **Russian Health Insurance Number**, **Russian Taxpayer Identification Number**, **Russian Main State Registration Number**, **Russian Classification Of Enterprises And Organizations**, **UK National Insurance Number**, **UK Phone Number**, **UK Post Code**, **UK Tax Code**, **URL**, **US Social Security Number**.
Condition:	Specificare le condizioni delle regole di attivazione associate a questo gruppo di contenuto. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Condition**:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	• **Less than or =** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è inferiore o uguale al numero specificato. • **Equal to** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è uguale al numero specificato. • **Greater than or =** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è superiore o uguale al numero specificato. • **Between** indica che una regola associata a questo gruppo di contenuto viene attivata tutte le volte che il numero di corrispondenze restituito dall'espressione comune è compreso nell'intervallo specificato.
Advanced	Verificare rapidamente il motivo dell'espressione comune su dati campione. Fare clic su **Advanced** per visualizzare o nascondere la casella **Test sample.**
Test sample	Inserire una stringa campione e visualizzare il risultato. DeviceLock supporta l'evidenziazione a colori in tempo reale dei risultati del test. Tutte le corrispondenze vengono evidenziate in verde, mentre le stringhe che non corrispondono al motivo vengono evidenziate in rosso.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Pattern Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Document Properties (Proprietà documenti)

I gruppi Document Properties consentono di controllare l'accesso ai file in base a proprietà dei file come nome e dimensione file, ecc. È inoltre possibile utilizzare un gruppo di contenuto Document Properties per controllare l'accesso a documenti e archivi protetti da password e immagini di testo.

Nota: la logica AND viene applicata a tutte le proprietà di file specificate in un gruppo Document Properties. Se, ad esempio, si desidera controllare l'accesso ai file di dimensioni superiori a 5 megabyte (MB) e ai documenti e agli archivi protetti da password, è necessario creare due gruppi Document Properties separati: uno per i file di dimensioni superiori a 5 MB e l'altro per i documenti e gli archivi protetti da password. Se queste proprietà di file vengono specificate nello stesso gruppo Document Properties e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà i documenti e gli archivi protetti da password di dimensioni superiori a 5 MB.

Non sono presenti gruppi di contenuto Document Properties predefiniti (incorporati). La seguente procedura descrive come creare gruppi Document Properties personalizzati.

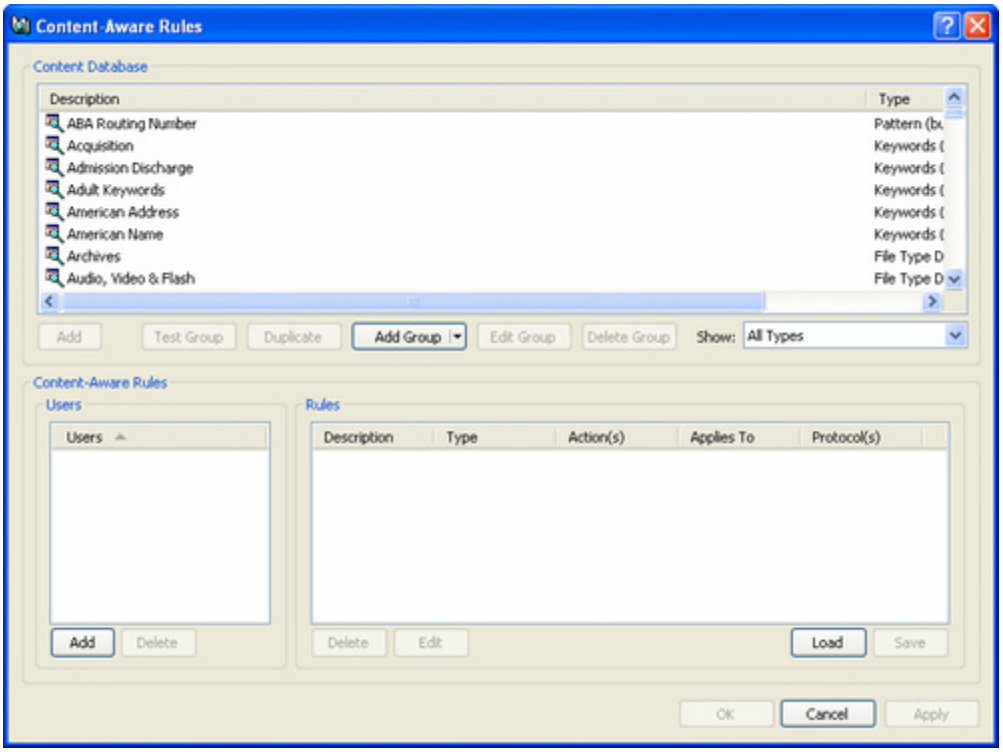
Per creare un gruppo Document Properties (Proprietà documenti)

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

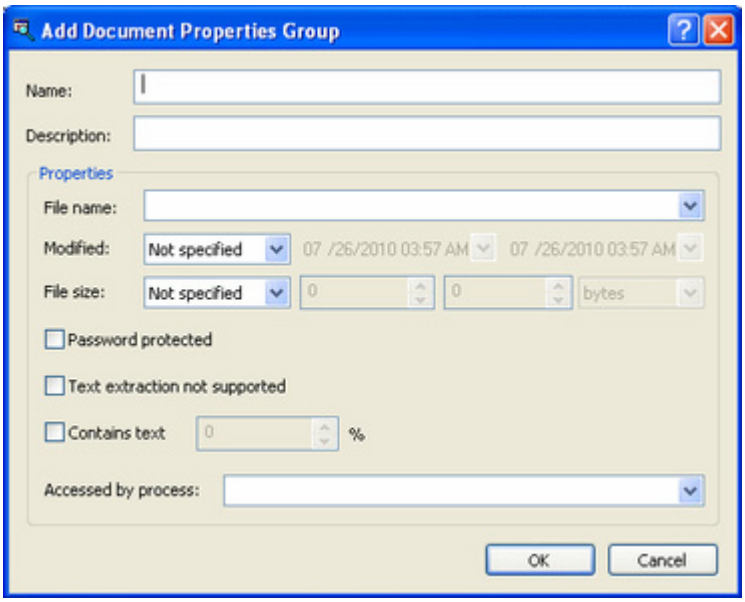
   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Document Properties**.

   Viene visualizzata la finestra di dialogo Add Document Properties Group.



5. Nella finestra di dialogo **Add Document Properties Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
File name	Specificare i nomi di file. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?). Ad esempio, digitare ***.txt** per specificare tutti i file con estensione .txt. I nomi di file multipli vanno separati da una virgola da un punto e virgola (;), ad esempio ***.doc; *.docx**. *Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere*.
Modified	Specificare l'ultima data/ora di modifica del file. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **Modified**: • **Not specified** (opzione predefinita) • **Before than** indica che la data/ora di modifica del file deve essere precedente alla data/ora specificata. • **After than** indica che la data/ora di modifica del file deve essere posteriore alla data/ora specificata. • **Between** indica che la data/ora di modifica del file deve rientrare nell'intervallo di date/ore specificato. • **Not older than** indica che la data/ora di modifica del file non

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	deve essere antecedente al numero specificato di secondi, minuti, giorni, settimane, mesi e anni. • **Older than** indica che la data/ora di modifica del file deve essere antecedente al numero specificato di secondi, minuti, giorni, settimane, mesi e anni. **Nota:** la proprietà **Modified** non si applica ai file trasmessi sulla rete. Se è stata specificata, viene ignorata durante l'analisi del contenuto.
File size	Specificare la dimensione del file in byte, kilobyte, megabyte, gigabyte o terabyte. Per farlo, selezionare una qualsiasi delle seguenti opzioni nell'elenco **File size**: • **Not specified** (opzione predefinita) • **Equal to** indica che la dimensione del(i) file deve corrispondere alla dimensione specificata. • **Less than** indica che la dimensione del(i) file deve essere inferiore alla dimensione specificata. • **More than** indica che la dimensione del(i) file deve essere superiore alla dimensione specificata. • **Between** indica che la dimensione del(i) file deve rientrare nell'intervallo specificato.
Password protected	Rilevare e controllare l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office (.doc, .xls, .ppt, .docx, .xlsx, .pptx) protetti da password. Se viene selezionata la casella di controllo **Password protected** per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office protetti da password. Deselezionare la casella di controllo **Password protected** se non si desidera rilevare e controllare l'accesso agli archivi, ai file PDF e ai documenti Microsoft Office protetti da password. Per informazioni sui formati di archivio supportati, consultare la descrizione della funzionalità "Ispezione di file all'interno di archivi".
Text extraction not supported	Controllare l'accesso ai formati di file non supportati. Se viene selezionata la casella di controllo **Text extraction not supported** per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto, la regola controllerà l'accesso a tutti i file di formati non supportati. Per visualizzare l'elenco completo dei file supportati, consultare la sezione "Estensione delle funzionalità di DeviceLock con ContentLock e NetworkLock".
Contains text	Rilevare e controllare l'accesso alle immagini in base della presenza di testo o meno all'interno di queste ultime. Se viene selezionata la casella di controllo **Contains text** per un gruppo Document Properties (Proprietà documenti) e, in seguito, si crea una regola basata sul contenuto (Content-Aware Rule) correlata a questo gruppo di contenuto e al gruppo di contenuto incorporato Images, CAD &

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	Drawing (File Type Detection: Rilevamento tipo file), la regola verificherà la presenza di testo nei file di immagine supportati e controllerà l'accesso alle immagini di testo. Deselezionare la casella di controllo **Contains text** se non si desidera rilevare e controllare l'accesso alle immagini di testo. Per informazioni sui file di immagine supportati, consultare la descrizione della funzionalità "Rilevamento di testo nelle immagini". Se viene selezionata la casella di controllo **Contains text**, specificare la quantità di testo contenuta nelle immagini. La quantità di testo viene espressa in termini percentuali rispetto all'area totale dell'immagine. Ad esempio, se il testo occupa la metà dell'immagine, la quantità di testo equivale al 50%. Se un'immagine contiene solo testo, la quantità di testo equivale al 100%. **Nota:** l'opzione **Contains text** si applica anche agli altri formati di file supportati. In questo caso, la percentuale indica il rapporto tra la dimensione del testo in caratteri e la dimensione del file in byte.
Accessed by process	Specificare il nome del processo che accede al file del documento. È possibile utilizzare caratteri jolly come gli asterischi (*) e i punti interrogativi (?). I nomi di processi multipli vanno separati da un punto e virgola (;), ad esempio **explorer.exe; notepad.exe**.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Document Properties Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Gruppi di contenuto Complex (Complessi)

I gruppi Complex ricorrono alle espressioni booleane per selezionare i dati per cui si desidera controllare l'accesso. Questi gruppi possono includere qualsiasi combinazione di gruppi di contenuto incorporati o personalizzati (File Type Detection, Keywords, Pattern e Document Properties) associati a qualsiasi numero di operatori logici standard. Ciascun gruppo di contenuto viene trattato come singolo criterio di filtro che può essere incluso nell'espressione booleana dell'utente. Utilizzando più gruppi di contenuto, è possibile creare filtri complessi al fine di identificare il contenuto dei dati trasmessi sulla rete.

La seguente tabella include gli operatori logici in ordine di preferenza, dal più elevato al più basso

OPERATORE	SIGNIFICATO
NOT	Negazione logica di un criterio di filtro

OPERATORE	SIGNIFICATO
AND	Entrambi i criteri di filtro vanno applicati
OR	Può essere applicato l'uno o l'altro criterio di filtro

È possibile utilizzare parentesi per modificare la precedenza degli operatori e forzare la valutazione di alcune parti di un'espressione prima di altre. I criteri nidificati inclusi tra parentesi vengono valutati nell'ordine dall'interno verso l'esterno. Sono supportati più livelli di nidificazione. Un gruppo complesso può contenere un massimo di 30 gruppi di contenuto.

Non sono presenti gruppi di contenuto Complex predefiniti (incorporati). La seguente procedura descrive come creare gruppi Complex personalizzati.

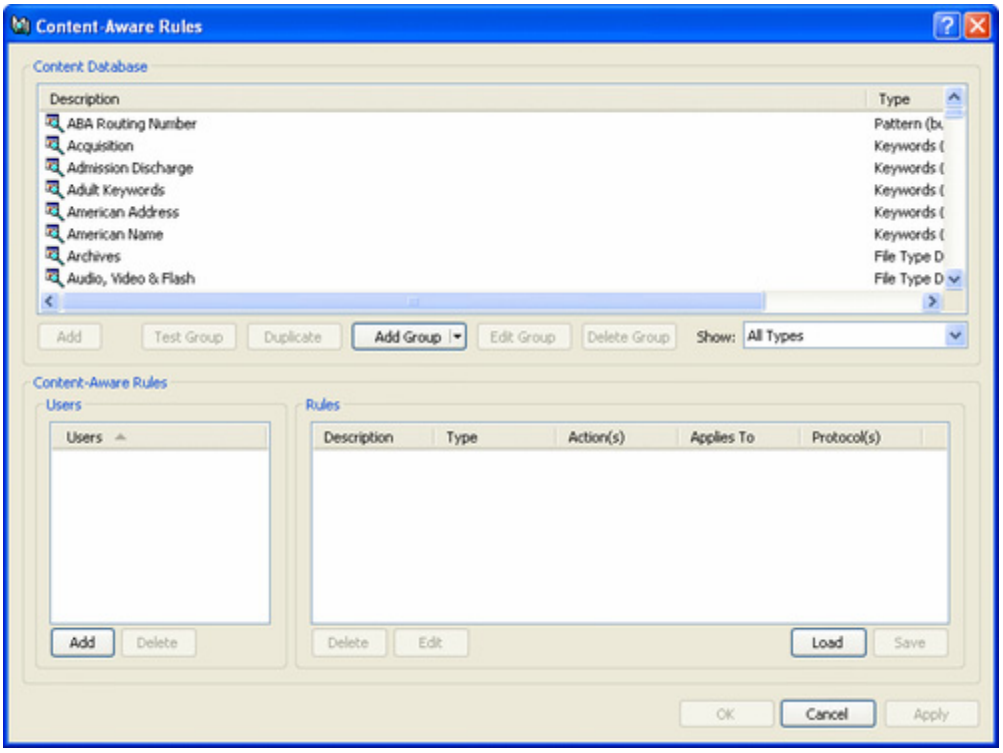
Per creare un gruppo Complex (Complessi)

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

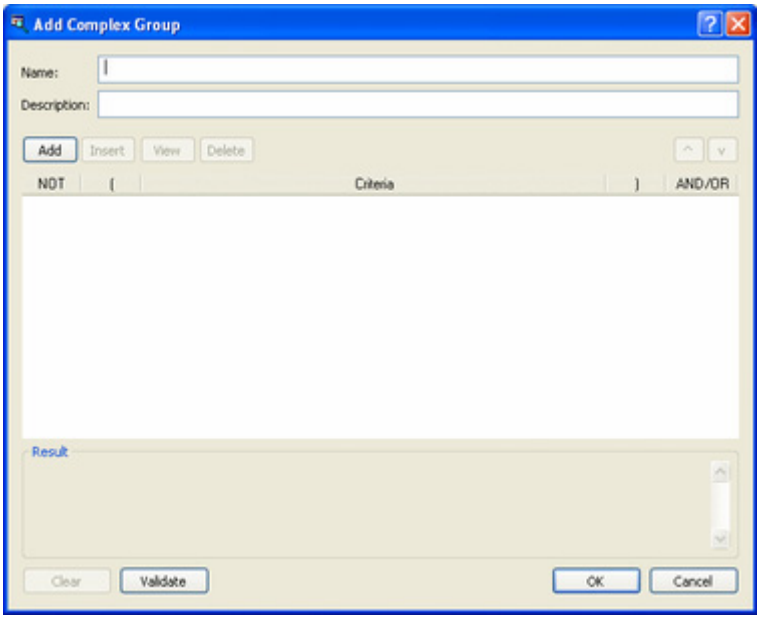
   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Complex**.

   Viene visualizzata la finestra di dialogo Add Complex Group.



5. Nella finestra di dialogo **Add Complex Group**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Name	Specificare il nome del gruppo.
Description:	Specificare una descrizione per il gruppo.
Add	Aggiungere i gruppi di contenuto desiderati selezionandoli dal database dei contenuti. Per farlo, fare clic su **Add** per aprire la finestra di dialogo **Content Groups**. Nella finestra di dialogo **Content Groups**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **OK**. *È possibile selezionare più gruppi di contenuto tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui gruppi*. *Per visualizzare le informazioni su un gruppo di contenuto, selezionare il gruppo desiderato e fare clic su View Group*. *I gruppi di contenuto aggiunti vengono visualizzati nella colonna Criteria della finestra di dialogo Add Complex group. Ciascun gruppo di contenuto aggiunto viene trattato come singolo criterio di filtro che può essere incluso nell'espressione booleana dell'utente*.
Insert	Inserire uno dei gruppi di contenuto inclusi nel database dei contenuti prima del gruppo correntemente selezionato nella colonna **Criteria**. Per farlo, fare clic su **Insert** per aprire la finestra di dialogo **Content Groups**. Nella finestra di dialogo **Content Groups**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **OK**.
View	Visualizzare informazioni sul gruppo correntemente selezionato nella colonna **Criteria**.
Delete	Eliminare il gruppo selezionato dalla colonna **Criteria**.
NOT	Associare a ciascun gruppo di contenuto selezionato un operatore logico NOT. Per farlo, selezionare il gruppo desiderato nella colonna **Criteria**, quindi scegliere la casella di controllo pertinente nella colonna **Not**.
AND/OR	Associare a ciascun gruppo di contenuto selezionato l'operatore logico AND od OR. Per farlo, selezionare il gruppo desiderato nella colonna **Criteria**, quindi fare clic su **AND** od **OR** nell'elenco appropriato nella colonna **AND/OR**.
Clear	Cancellare l'elenco corrente dei gruppi di contenuto nella colonna **Criteria**.
Validate	Convalidare l'espressione. Se l'espressione è stata definita in maniera incorretta (ad esempio, una parentesi aperta non è stata accompagnata da una parentesi chiusa), viene visualizzato un messaggio di errore.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Add Complex Group**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo

Content-Aware Rules.

Visualizzazione dei gruppi di contenuto incorporati

È possibile visualizzare tutti i gruppi di contenuto incorporati, ma non modificarli né eliminarli.

Per visualizzare un gruppo di contenuto incorporato

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Service Settings Editor:
    a) Aprire DeviceLock Service Settings Editor.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Group Policy Manager:
    a) Aprire Group Policy Object Editor.
    b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
    - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
      - OPPURE -
    - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

    Viene visualizzata la finestra di dialogo Content-Aware Rules.
4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo incorporato da visualizzare, quindi fare clic su **View Group**.

Duplicazione dei gruppi di contenuto incorporati

Non è possibile modificare i gruppi di contenuto incorporati, mentre si possono creare e utilizzare copie modificabili di questi ultimi (duplicati) in base alle esigenze della propria organizzazione.

Per duplicare un gruppo di contenuto incorporato

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
    b) Nella struttura della console, espandere **DeviceLock Service**.

    Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere Computer Configuration, quindi DeviceLock.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare il gruppo di contenuto incorporato che si desidera duplicare, quindi fare clic su **Duplicate**.
5. Nella finestra di dialogo visualizzata, apportare le modifiche desiderate al gruppo di contenuto, quindi fare clic su **OK**.

   Il gruppo di contenuto appena creato viene aggiunto all'elenco dei gruppi di contenuto, sotto Content Database, nel riquadro superiore della finestra di dialogo Content-Aware Rules.

Modifica ed eliminazione dei gruppi di contenuto personalizzati

È possibile modificare o eliminare i gruppi di contenuto personalizzati in qualsiasi momento.

Per modificare o eliminare un gruppo di contenuto personalizzato

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi DeviceLock.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.

  - OPPURE -

- Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo di contenuto da modificare o eliminare.
5. Fare clic su **Edit Group** per modificare il gruppo di contenuto selezionato. Nella finestra di dialogo visualizzata, apportare le modifiche desiderate, quindi fare clic su **OK**.

   - OPPURE -

   Fare clic su **Delete Group** o premere il tasto CANC per eliminare il gruppo di contenuto selezionato.
6. Nella finestra di dialogo **Content-Aware Rules**, fare clic su **OK** o **Apply** per applicare le modifiche.

Verifica dei gruppi di contenuto

È possibile verificare qualsiasi gruppo di contenuto incorporato o personalizzato per vedere se i file specificati corrispondono allo stesso. Grazie a questo tipo di test, è possibile verificare il rispetto dei propri requisiti aziendali specifici da parte delle regole create in base ai gruppi di contenuto.

Per verificare un gruppo di contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.

     - OPPURE -

- Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare qualsiasi gruppo incorporato da verificare, quindi fare clic su **Test Group**.

   È possibile verificare un solo gruppo alla volta.

   Viene visualizzata la finestra di dialogo Open.

5. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da utilizzare per verificare il gruppo di contenuto specificato.
6. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
7. Fare clic sul file, quindi scegliere **Open**.

   Viene visualizzata la finestra di messaggio Result. Se il file corrisponde al gruppo di contenuto specificato, nella finestra di messaggio Result viene visualizzata la seguente frase: "Selected file matches with the group". Se il file non corrisponde al gruppo di contenuto specificato, nella finestra di messaggio Result viene visualizzata la seguente frase: "Selected file does not match with the group".

   Durante la verifica, la console non risponde ai comandi (si blocca).

Gestione delle regole basate sul contenuto

La gestione delle Content-Aware Rules (regole basate sul contenuto) include le seguenti attività:

- Definizione delle regole basate sul contenuto
- Modifica delle regole basate sul contenuto
- Copia delle regole basate sul contenuto
- Esportazione e importazione delle regole basate sul contenuto
- Rimozione della definizione delle regole basate sul contenuto
- Eliminazione delle regole basate sul contenuto

È possibile gestire le regole basate sul contenuto utilizzando DeviceLock Management Console, DeviceLock Group Policy Manager o DeviceLock Service Settings Editor.

Definizione delle regole basate sul contenuto

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto incorporati o personalizzati. Per informazioni dettagliate su questi gruppi, consultare la sezione "Configurazione delle impostazioni di rilevamento del contenuto".

Per definire una regola basata sul contenuto (Content-Aware Rule)

1. Se si utilizza DeviceLock Management Console:

a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

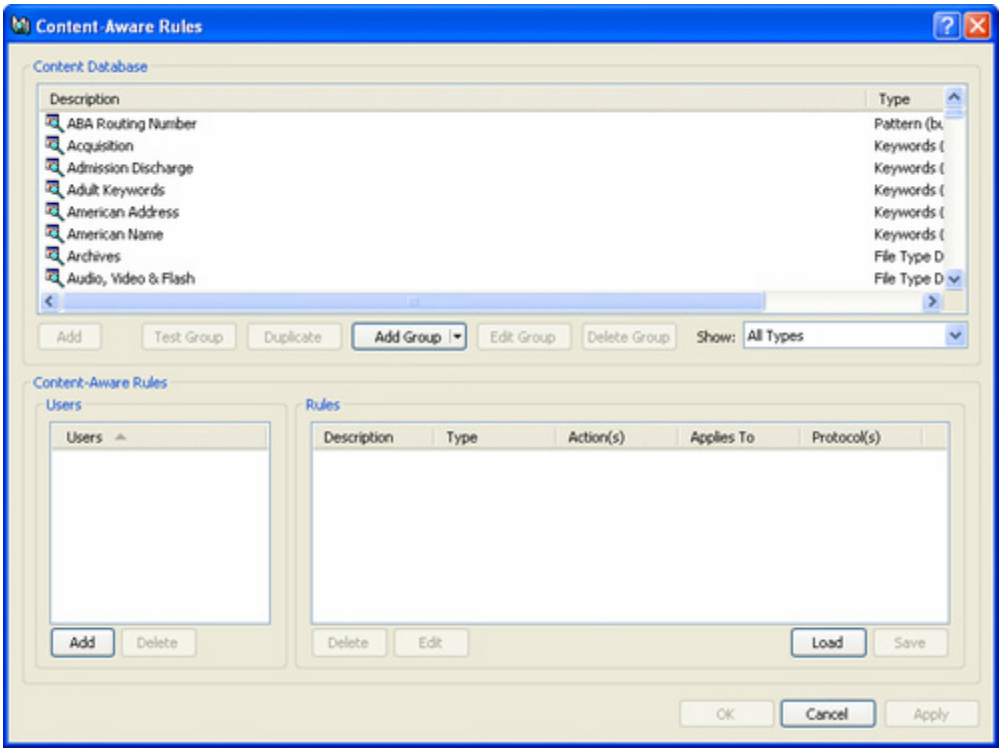
a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.



4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la regola, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules.

   Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

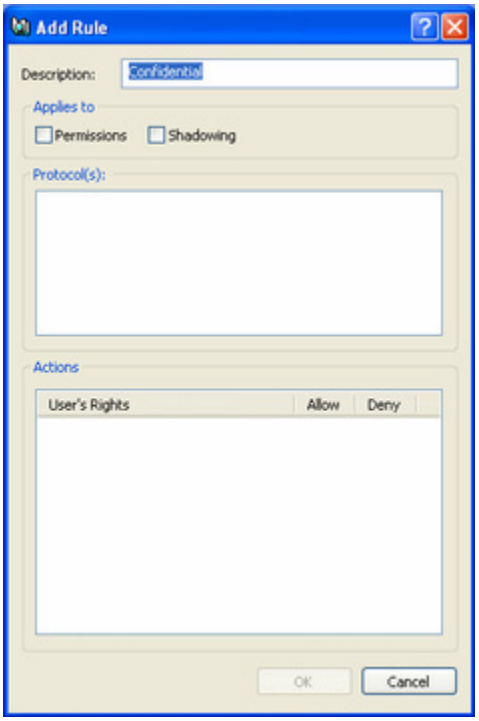
6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare gli utenti o i gruppi per cui si desidera definire la regola.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

7. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **Add**.

   Nota: è possibile specificare un solo gruppo di contenuto per ogni regola basata sul contenuto.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, nella casella **Description**, digitare il nome della regola basata sul contenuto.

   Per impostazione predefinita, quest'ultima ha lo stesso nome del gruppo di contenuto specificato, ma è possibile specificare un altro nome.

9. Sotto **Applies to**, specificare il tipo di operazione associata alla regola. Le opzioni disponibili sono:

- **Permissions**: specifica che la regola verrà applicata alle operazioni di controllo dell'accesso.
- **Shadowing**: specifica che la regola verrà applicata alle operazioni di copia shadow.
- **Permissions, Shadowing**: specifica che la regola verrà applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.

10. Sotto **Protocol(s)**, selezionare i protocolli appropriati a cui si desidera applicare la regola.

    Le regole basate sul contenuto possono essere applicate ai seguenti protocolli: FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, Social Networks, Web Mail, Windows Messenger e Yahoo Messenger.

    Se vengono selezionati più protocolli con diversi diritti di accesso, nella finestra di dialogo sotto Action(s) vengono visualizzati solo i diritti di accesso comuni per tutti i protocolli selezionati.

11. Sotto **Action(s)**, specificare quali azioni degli utenti sono autorizzate o non autorizzate per i protocolli e quali azioni degli utenti vanno inserite in Shadow Log.

    Per informazioni dettagliate sui diritti degli utenti che possono essere specificati nelle regole basate sul contenuto (Content-Aware Rules), consultare le sezioni "Regole basate sul contenuto per le operazioni di controllo dell'accesso" e "Regole basate sul contenuto per le operazioni di copia shadow".

12. Fare clic su **OK**.

    La regola creata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules.

13. Fare clic su **OK** o su **Apply** per applicare la regola.

    Gli utenti o i gruppi per cui è stata applicata la regola basata sul contenuto vengono visualizzati sotto Content-Aware Rules nella struttura della console. Se nella struttura della console viene selezionato un utente o un gruppo per cui è stata applicata una regola basata sul contenuto, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:

    - **Description**: il nome della regola. Per impostazione predefinita, la regola ha lo stesso nome del gruppo di contenuto specificato.
    - **Type**: il tipo di analisi del contenuto. Valori possibili: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties** e **Complex**. **File Type Detection** indica che il riconoscimento e l'identificazione dei file si basa sulle loro firme caratteristiche. **Keywords** indica che il riconoscimento e l'identificazione dei file/dati si basa sulle parole chiave o frasi specificate. **Pattern** indica che il riconoscimento e l'identificazione dei file/dati si basa sui motivi di testo specificati descritti dalle espressioni comuni Perl. **Document Properties** indica che il riconoscimento e l'identificazione dei file si basa sulle loro proprietà. **Complex** indica che il riconoscimento e l'identificazione dei file/dati si basa sul contenuto specificato descritto da un'espressione booleana.
    - **Action(s)**: mostra quali azioni degli utenti sono autorizzate o non autorizzate per i protocolli e quali azioni degli utenti vanno inserite in Shadow Log.
    - **Applies To**: Valori possibili: **Permissions**, **Shadowing** e **Permissions, Shadowing**. **Permissions** indica che la regola viene applicata alle operazioni

di controllo dell'accesso. **Shadowing** indica che la regola viene applicata alle operazioni di copia shadow. **Permissions, Shadowing** indica che la regola viene applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.

- **Protocol(s)**: i protocolli per cui viene applicata la regola.
- **Profile**: Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

  È possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire le regole basate sul contenuto offline per i protocolli, consultare la sezione "Gestione delle regole basate sul contenuto offline per i protocolli".

Modifica delle regole basate sul contenuto

È possibile modificare le proprietà delle regole basate sul contenuto (Content-Aware Rule) come Description, Applies To, Protocol(s) e Actions.

Come modificare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, scegliere **Manage**, quindi attenersi alla procedura seguente:

   a) Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

   b) Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.

   - OPPURE -

   Fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Edit** nel menu di scelta rapida.

   - OPPURE -

   Sotto **Protocols**, espandere **Content-Aware Rules**, quindi attenersi alla procedura seguente:

a) Sotto **Content-Aware Rules**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto applicati agli stessi nel riquadro dei dettagli.

b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.

- OPPURE -

Nel riquadro dei dettagli, fare doppio clic sulla regola che si desidera modificare.

Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare le proprietà della regola a seconda delle proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole basate sul contenuto

Per riutilizzare le regole basate sul contenuto (Content-Aware Rules) esistenti, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Come copiare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**.

     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules.

4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

5. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. Se si usa la combinazione di tasti CTRL+X, la regola viene tagliata solo dopo essere stata incollata.

   Per eseguire un'operazione di trascinamento, selezionare la regola e spostarla verso l'utente o il gruppo a cui si desidera applicare la regola copiata.

6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi a cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules.

8. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare gli utenti o i gruppi a cui applicare la regola copiata.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

9. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, fare clic con il pulsante destro del mouse sul riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules.

10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione delle regole basate sul contenuto

È possibile esportare tutte le Content-Aware Rules (regole basate sul contenuto) correnti in un file .cwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare le regole basate sul contenuto

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Save**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Save** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo a cui viene applicata la regola, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Save** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .cwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   Le regole esportate vengono salvate in un file con estensione .cwl.

Come importare le regole basate sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Load**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Load** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo a cui viene applicata la regola, quindi scegliere **Load**.
     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Load**.
     - OPPURE -
   - Espandere Content-Aware Rules, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Load** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, fare clic su **Load**.

   Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   È possibile importare un solo file .cwl alla volta.

Rimozione della definizione delle regole basate sul contenuto

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che le regole basate sul contenuto vengano applicate a un gruppo specifico di computer client. Per farlo, occorre riportare le regole basate sui contenuti precedentemente definite al loro stato non configurato. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Come rimuovere la definizione delle regole basate sul contenuto

1. Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
c) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Undefine**.

Eliminazione delle regole basate sul contenuto

Quando alcune Content-Aware Rules (regole basate sul contenuto) non sono più necessarie, possono essere eliminate.

Come eliminare una regola basata sul contenuto

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo a cui viene applicata la regola, quindi scegliere **Delete user**.

     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.

     - OPPURE -

   - Espandere **Content-Aware Rules** e selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.

     - OPPURE -

- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage**. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.

  È possibile selezionare più regole da eliminare tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sulle regole.

Protocolli (Regular Profile)

DeviceLock consente di controllare i dati trasferiti su diversi protocolli di rete, migliorando in tal modo la protezione contro la divulgazione involontaria delle informazioni e la sicurezza a livello di trasporto. La funzionalità Protocols consente di definire criteri in grado di autorizzare o bloccare in maniera selettiva la trasmissione di dati/file attraverso determinati protocolli e l'esecuzione della copia shadow per i dati trasferiti. I criteri sono flessibili e possono essere definiti a livello di utente o di gruppo.

DeviceLock assicura il controllo sui seguenti protocolli e applicazioni Web:

- **FTP** (File Transfer Protocol): protocollo di Internet standard per il trasferimento di file tra più computer.
  Sono supportate le connessioni FTP in modalità attiva e passiva. Viene supportato anche FTPS (FTP su SSL). Sono supportate le connessioni FTPS implicite ed esplicite.
- **HTTP** (Hypertext Transfer Protocol): protocollo client/server a livello di applicazione utilizzato per trasferire le informazioni sul World Wide Web.
  Viene supportato anche HTTPS (SSL su HTTP).
- **ICQ/AOL Messenger**: protocollo OSCAR (Open System for Communication in Realtime) di AOL utilizzato da ICQ e AOL Instant Messenger (AIM).
  Sono supportate le connessioni non-SSL e SSL.
- **IRC** (Internet Relay Chat): protocollo standard di Internet che supporta le comunicazioni interattive, in tempo reale e basate su testo che si svolgono nelle "chat room" affermate su Internet attraverso i server IRC.
  Sono supportate le connessioni non-SSL e SSL.
- **Jabber**: protocollo aperto e basato su XML per la messaggistica immediata.
  Sono supportate le connessioni non-SSL e SSL.
- **Mail.ru Agent**: programma di messaggistica immediata creato da Mail.ru.
- **SMTP** (Simple Mail Transfer Protocol): protocollo standard di Internet utilizzato per lo scambio di messaggi e-mail tra server SMTP su Internet.
  Viene supportato anche l'SMTP esteso (ESMTP). Sono supportate le connessioni non-SSL e SSL.
- **Social Networks**: controlla le comunicazioni con i siti di reti sociali. Sono supportati i seguenti siti di reti sociali: Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING.

  Nota: il traffico SSL dei siti di reti sociali viene controllato come traffico generico (non-SSL).
- **Telnet**: protocollo di Internet standard per il servizio di connessione al terminale remoto.
- **Web Mail**: controlla le comunicazioni e-mail basate sul Web. Sono supportati i seguenti servizi e-mail basati sul Web: AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru, Rambler Mail, Web.de, Yahoo! Mail, et Yandex Mail.

Sono supportate le connessioni non-SSL e SSL.

- **Windows Messenger**: MSNP (Microsoft Notification Protocol) è il principale protocollo utilizzato da Windows Live Messenger e Windows Messenger.
- **Yahoo Messenger**: il principale protocollo di rete utilizzato dal client di messaggistica immediata Yahoo! Messenger.

Nota: il protocollo SSL viene utilizzato nella lista bianca dei protocolli per autorizzare le applicazioni con certificati SSL incorporati a collegarsi con il proprio server.

È possibile gestire i criteri di protezione dei protocolli utilizzando DeviceLock Management Console, Service Settings Editor o DeviceLock Group Policy Manager. È inoltre possibile utilizzare il plug-in Report Permissions/Auditing di DeviceLock Enterprise Server per visualizzare e modificare i criteri di protezione definiti per i protocolli. Per ulteriori informazioni, consultare la sezione "Report Permissions/Auditing".

Gestione delle autorizzazioni per i protocolli

Per gestire lo scambio di informazioni a livello di trasporto, occorre configurare l'accesso ai protocolli delle comunicazioni impostando le autorizzazioni adeguate. Queste ultime consentono di specificare chi può accedere a quali protocolli e i livelli di accesso degli utenti. Le autorizzazioni possono essere definite a livello di utente o di gruppo.

La seguente tabella descrive i diritti di accesso disponibili per le autorizzazioni associate ai protocolli.

PROTOCOLLO	DIRITTI DI ACCESSO
FTP	**Generic: Send/Receive Data** Diritto di collegarsi a un server FTP, inviare e ricevere dati di protocollo, scaricare file da un server FTP. **Generic: Outgoing Files** Diritto di caricare file su un server FTP. **SSL: Send/Receive Data** Diritto di collegarsi a un server FTP, inviare e ricevere dati di protocollo, scaricare file da un server FTP utilizzando FTPS. **SSL: Outgoing Files** Diritto di caricare file su un server FTP utilizzando FTPS.
HTTP	**Generic: Send/Receive Data** Diritto di collegarsi a un server Web, inviare e ricevere dati di protocollo, pagine Web e oggetti di queste ultime (ad esempio script, file Flash e immagini JPEG, PNG e GIF, ecc.). **Generic: POST Requests** Diritto di inviare dati di moduli Web su un Server Web utilizzando HTTP. **Generic: Outgoing Files** Diritto di caricare file su un server Web utilizzando HTTP. **SSL: Send/Receive Data** Diritto di collegarsi a un server Web, inviare e ricevere dati di protocollo, pagine Web e oggetti di queste ultime (ad esempio script, file Flash e immagini JPEG, PNG e GIF, ecc.) utilizzando HTTPS. **SSL: POST Requests** Diritto di inviare dati di moduli Web su un Server Web utilizzando HTTPS.

PROTOCOLLO	DIRITTI DI ACCESSO
	SSL: Outgoing Files Diritto di caricare file su un server Web utilizzando HTTPS.
ICQ/AOL Messenger	**Generic: Send/Receive Data** Diritto di collegarsi al server di ICQ e AOL Instant Messenger e ricevere messaggi immediati. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file. **SSL: Send/Receive Data** Diritto di collegarsi al server di ICQ e AOL Instant Messenger e ricevere messaggi immediati utilizzando SSL. **SSL: Outgoing Messages** Diritto di inviare messaggi immediati utilizzando SSL. Non controlla i trasferimenti di file.
IRC	**Generic: Send/Receive Data** Diritto di collegarsi a un server IRC e ricevere messaggi immediati. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file. **SSL: Send/Receive Data** Diritto di collegarsi a un server IRC utilizzando SSL. **SSL: Outgoing Messages** Diritto di inviare messaggi immediati utilizzando SSL. Non controlla i trasferimenti di file.
Jabber	**Generic: Send/Receive Data** Diritto di collegarsi a un server Jabber e ricevere messaggi immediati. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file. **SSL: Send/Receive Data** Diritto di collegarsi a un server Jabber utilizzando SSL. **SSL: Outgoing Messages** Diritto di inviare messaggi immediati utilizzando SSL. Non controlla i trasferimenti di file.
Mail.ru Agent	**Generic: Send/Receive Data** Diritto di collegare Mail.ru Agent al server Mail.ru e ricevere messaggi immediati. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file.
SMTP	**Generic: Send/Receive Data** Diritto di collegarsi a un server SMTP e inviare e ricevere dati di protocollo. **Generic: Outgoing Messages** Diritto di inviare messaggi e-mail senza allegati. **Generic: Outgoing Files** Diritto di inviare allegati e-mail. **SSL: Send/Receive Data** Diritto di collegarsi a un server SMTP e inviare e ricevere dati di protocollo utilizzando SSL. **SSL: Outgoing Messages** Diritto di inviare messaggi e-mail senza allegati utilizzando SSL. **SSL: Outgoing Files** Diritto di inviare allegati e-mail utilizzando SSL.
Social Networks	**Generic: Send/Receive Data** Diritto di accedere al sito di una rete sociale in modalità di visualizzazione. **Generic: Outgoing Messages** Diritto di inviare messaggi, commenti, post, ecc. **Generic: Outgoing Files** Diritto di caricare file multimediali e contenuti sul sito di una rete sociale.

PROTOCOLLO	DIRITTI DI ACCESSO
Telnet	**Generic: Send/Receive Data** Diritto di collegarsi a un server Telnet e inviare e ricevere dati di protocollo.
Web Mail	**Generic: Send/Receive Data** Diritto di accedere alla Webmail e leggere la posta elettronica. **Generic: Outgoing Messages** Diritto di inviare messaggi e-mail senza allegati. **Generic: Outgoing Files** Diritto di inviare allegati e-mail. **SSL: Send/Receive Data** Diritto di accedere alla Webmail e leggere la posta elettronica utilizzando SSL. **SSL: Outgoing Messages** Diritto di inviare messaggi e-mail senza allegati utilizzando SSL. **SSL: Outgoing Files** Diritto di inviare allegati e-mail utilizzando SSL.
Windows Messenger	**Generic: Send/Receive Data** Diritto di collegarsi al server di Windows Messenger. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file.
Yahoo Messenger	**Generic: Send/Receive Data** Diritto di collegarsi al server di Yahoo Messenger. **Generic: Outgoing Messages** Diritto di inviare messaggi immediati. Non controlla i trasferimenti di file.

Nota: è possibile definire più autorizzazioni online od offline per i protocolli per lo stesso utente o gli stessi gruppi di utenti. Le autorizzazioni online (Regular Profile) si applicano ai computer client che operano online. Le autorizzazioni offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire le autorizzazioni offline per i protocolli, consultare la sezione "Gestione delle autorizzazioni offline per i protocolli".

È possibile impostare le autorizzazioni predefinite per i protocolli per entrambi i tipi di profilo (Regular Profile e Offline Profile). Le autorizzazioni predefinite sono assegnate agli account Administrators ed Everyone. La seguente tabella illustra i diritti di accesso concessi a questi account per impostazione predefinita.

ACCOUNT/ PROTOCOLLO	ADMINISTRATORS	EVERYONE
FTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data SSL: Send/Receive Data
HTTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing	Generic: Send/Receive Data SSL: Send/Receive Data

ACCOUNT/ PROTOCOLLO	ADMINISTRATORS	EVERYONE
	Files	
ICQ/AOL Messenger	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
IRC	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Jabber	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Mail.ru Agent	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages
SMTP	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Social Networks	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Telnet	Generic: Send/Receive Data	Generic: Send/Receive Data
Web Mail	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
Windows Messenger	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages
Yahoo Messenger	Generic: Send/Receive Data, Outgoing Messages	Generic: Send/Receive Data, Outgoing Messages

La gestione delle autorizzazioni online (regolari) per i protocolli include le seguenti attività:

- Impostazione e modifica delle autorizzazioni
- Rimozione della definizione delle autorizzazioni

Le autorizzazioni online per i protocolli possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le autorizzazioni per un protocollo non sono state configurate.

STATO	DESCRIZIONE
Configured	Indica che le autorizzazioni per un protocollo sono state configurate.
Full Access	Indica che i diritti di accesso completi sono concessi all'account Everyone.
No Access	Indica una delle seguenti condizioni: • L'account Everyone dispone delle autorizzazioni di tipo No Access ed è l'unico account assegnato a un protocollo. *Le autorizzazioni No Access assegnate all'account Everyone hanno la priorità sulle autorizzazioni assegnate agli altri account.* • Tutti gli utenti e i gruppi assegnati a un protocollo hanno le autorizzazioni di tipo No Access. • Tutti gli utenti e i gruppi assegnati a un protocollo sono stati rimossi.

Impostazione e modifica delle autorizzazioni

Per impostare e modificare le autorizzazioni

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Permissions**.

   Dopo aver selezionato Permissions nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile impostare le autorizzazioni. Nella colonna Regular del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni online (regolari) per ciascun protocollo.
4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse sul protocollo per cui si desidera impostare o modificare le autorizzazioni, quindi scegliere **Set Permissions**.
     - OPPURE -
   - Selezionare il protocollo per cui si desidera impostare o modificare le autorizzazioni, quindi fare clic su **Set Permissions** sulla barra degli strumenti.

   È possibile selezionare più protocolli per cui impostare le stesse autorizzazioni tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui protocolli.

Nota: durante la selezione di più protocolli con diversi diritti di accesso, considerare quanto segue:

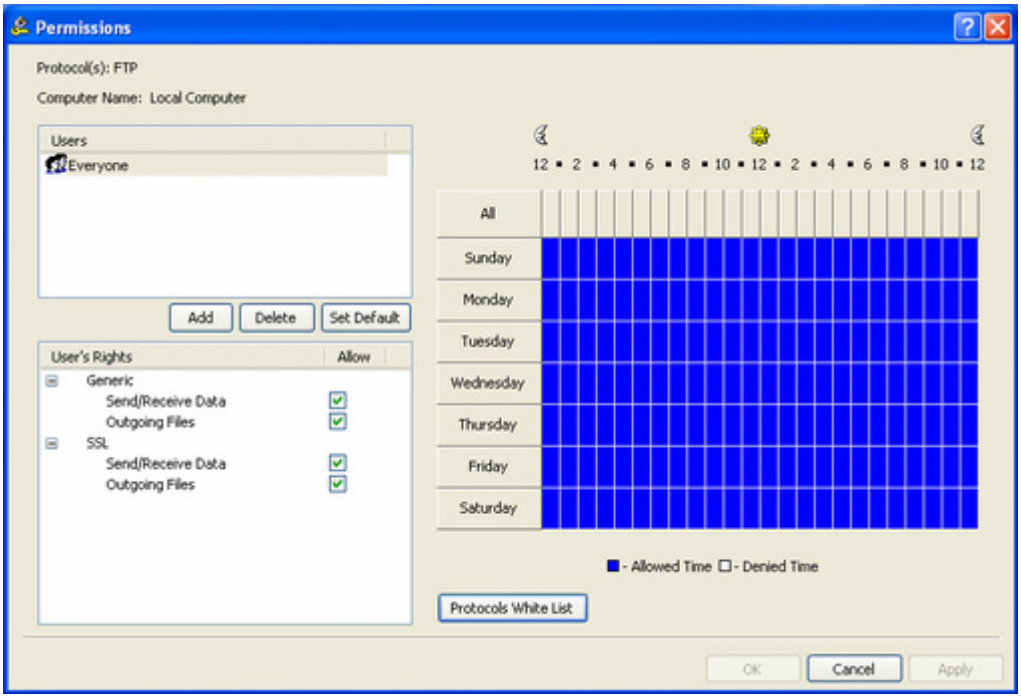
Nella finestra di dialogo **Permissions** vengono visualizzati solo i diritti di accesso comuni a tutti i protocolli selezionati.

Se tutti i diritti di accesso visualizzati nella finestra di dialogo **Permissions** sono stati concessi agli utenti specificati, questi ultimi disporranno dell'accesso completo ai protocolli selezionati.

Se tutti i diritti di accesso visualizzati nella finestra di dialogo **Permissions** sono stati negati agli utenti specificati, questi ultimi non potranno accedere ai protocolli selezionati.

Alcuni diritti di accesso dipendono da altri diritti. Se viene concesso un diritto che richiede un altro diritto, il diritto richiesto viene concesso automaticamente. Ad esempio, se viene concesso unicamente il diritto **Generic: Outgoing Files** per i protocolli Social Networks e Web Mail, i seguenti diritti vengono concessi automaticamente: **Generic: Send/Receive Data**, **Generic: Outgoing Messages**, **Generic: Outgoing Files**.

Viene visualizzata la finestra di dialogo Permissions.



5. Nella finestra di dialogo **Permissions**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Impostare le autorizzazioni predefinite	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**. *Le autorizzazioni predefinite sono assegnate agli account Administrators ed Everyone. Per informazioni sulle autorizzazioni assegnate a questi account per impostazione predefinita, consultare la sezione* "Gestione delle autorizzazioni per i protocolli".

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Impostare le autorizzazioni per un ulteriore utente o gruppo	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 2. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Permissions*. 3. Nel riquadro superiore sinistro della finestra di dialogo **Permissions**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti e/o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi*. 4. Nel riquadro inferiore sinistro della finestra di dialogo **Permissions**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati. *Nel riquadro destro della finestra di dialogo Permissions, è possibile impostare le restrizioni per data e ora, al fine di limitare l'accesso ai protocolli specificati da parte dell'utente. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui l'utente o il gruppo selezionato può accedere ai protocolli specificati. Utilizzare il pulsante destro del mouse per contrassegnare i giorni e le ore in cui l'utente o il gruppo selezionato non può accedere ai protocolli specificati*.
Modificare le autorizzazioni per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati.
Rimuovere un utente o gruppo esistente e le autorizzazioni	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle autorizzazioni

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che una parte o la totalità delle autorizzazioni precedentemente impostate per i protocolli venga applicata a un gruppo specifico di computer client. Per farlo, occorre reimpostare lo stato non configurato per le autorizzazioni precedentemente impostate. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Per rimuovere la definizione delle autorizzazioni

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
   c) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Permissions**.

   Dopo aver selezionato Permissions nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile impostare le autorizzazioni.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere la definizione delle autorizzazioni, quindi scegliere **Undefine**.

   È possibile rimuovere simultaneamente la definizione delle autorizzazioni per più protocolli. Per farlo, attenersi alle seguenti istruzioni:
   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui protocolli.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine**.

Gestione delle regole di controllo e shadowing per i protocolli

DeviceLock consente di controllare ed eseguire la copia shadow dei trasferimenti di dati/file eseguiti tramite diversi protocolli. Il controllo e la copia shadow vengono utilizzati per monitorare e registrare le operazioni di trasferimento dati critiche dal punto di vista della protezione. L'analisi regolare dei dati di registro è un metodo efficace per rilevare e monitorare gli utilizzi impropri di dati riservati e le violazioni delle norme sui dati provocate da perdite o furti di dati.

Per il controllo e la copia shadow a livello di trasporto, DeviceLock utilizza due tipi di registri: Audit Log e Shadow Log. Audit Log viene utilizzato per controllare l'accesso ai protocolli e monitorare i singoli utenti che effettuano l'accesso. I dati di controllo possono essere scritti su Windows Event Log, nel registro proprietario di DeviceLock o su entrambi. Per definire il registro da utilizzare, configurare il parametro Audit log type in Service Options. Per visualizzare i dati di Audit Log, utilizzare DeviceLock Service Audit Log Viewer o DeviceLock Enterprise Server Audit Log Viewer.

Shadow Log viene utilizzato per memorizzare una copia completa dei dati/file trasferiti tramite i protocolli specificati. Per visualizzare i dati di Shadow Log, utilizzare DeviceLock Service Shadow Log Viewer o DeviceLock Enterprise Server Shadow Log Viewer.

Il controllo e la copia shadow dei dati trasferiti tramite i protocolli specificati vengono attivati definendo le regole di controllo e di shadowing. Ciascuna regola associata a un protocollo specifica gli utenti o i gruppi cui viene applicata la regola e i diritti di controllo/shadowing appropriati che determinano le azioni degli utenti da controllare/sottoporre a copia shadow.

Gli eventi di controllo registrati includono informazioni come il tipo di evento, la data e l'ora dell'evento, il protocollo associato, l'utente associato con l'evento e dati sul processo e sull'evento.

La seguente tabella fornisce un riepilogo dei diritti di controllo e di shadowing che possono essere specificati nelle regole e dei dati sull'evento inseriti nel registro.

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
FTP	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi a un sito FTP. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro.* **Audit: Incoming Files -** attiva la registrazione del controllo dei tentativi degli utenti di scaricare un file da un sito FTP. *Nel registro vengono scritti l'azione Incoming File, il percorso assoluto e il nome completo del file (ad esempio ftp://mioftp/miofile.doc), l'indirizzo IP con il numero di porta e il nome dell'host.* **Audit: Outgoing Files -** attiva la registrazione del controllo dei tentativi degli utenti di caricare un file su un sito FTP. *Nel registro vengono scritti l'azione Outgoing File, il percorso assoluto e il nome completo del file (ad esempio ftp://mioftp/miofile.doc), l'indirizzo IP con il numero di porta e il nome dell'host.* **Shadowing: Incoming Files -** attiva la copia shadow dei file scaricati da un sito FTP. *Nel registro vengono scritte le copie shadow dei file scaricati.* **Shadowing: Outgoing Files -** Nel registro vengono scritte le copie shadow dei file scaricati. *Nel registro vengono scritte le copie shadow dei file caricati.*
HTTP	**Audit: Connection -** attiva la registrazione del controllo dei tentativi degli utenti di aprire una pagina Web. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro.* **Nota:** se viene attivato questo diritto, più eventi Connection vengono registrati

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
	nell'Audit Log tutte le volte che un utente cerca di aprire una pagina Web, poiché quest'ultima richiede spesso risorse (ad esempio immagini, script, ecc.) di altri host. **Audit: Incoming Data** - attiva la registrazione del controllo delle pagine Web e degli oggetti contenuti nelle stesse: script, file Flash (fino a 1,5 MB), immagini (fino a 512 KB), testo (fino a 200 KB) e così via. *Nel registro vengono scritti l'azione Incoming Data, l'URL della pagina e degli oggetti Web, l'indirizzo IP con il numero di porta e il nome dell'host*. **Audit: Incoming Files -** attiva la registrazione del controllo dei tentativi degli utenti di scaricare un file da un sito Web. *Nel registro vengono scritti l'azione Incoming File, il percorso assoluto e il nome completo del file (ad esempio http://dominio/percorso/miofile.doc), l'indirizzo IP con il numero di porta e il nome dell'host*. **Audit: Outgoing Data -** Il tipo di contenuto Outgoing Data non contiene dati. Questo diritto attiva la registrazione del controllo dei tentativi di apertura di una pagina Web eseguiti da utenti bloccati quando l'opzione **Audit Denied** è impostata per il protocollo. *Nel registro vengono scritti l'azione Outgoing Data, l'URL della pagina e degli oggetti Web, l'indirizzo IP con il numero di porta e il nome dell'host*. **Audit: POST Requests -** attiva la registrazione del controllo dei tentativi dell'utente di inviare a un sito Web dati di un modulo online. *Nel registro vengono scritti l'azione POST Request e l'URL dello script che ha inviato la richiesta POST*. **Audit: Outgoing Files -** attiva la registrazione del controllo dei tentativi degli utenti di caricare un file su un sito Web. *Nel registro vengono scritti l'azione Outgoing File, il percorso assoluto e il nome completo del file (ad esempio http://dominio/percorso/miofile.doc), l'indirizzo IP con il numero di porta e il nome dell'host*. **Shadowing: Incoming Data -** attiva la copia shadow delle pagine Web e degli oggetti contenuti nelle stesse: script, file Flash (fino a 1,5 MB), immagini (fino a 512 KB), testo (fino a 200 KB) e così via. *Le copie shadow delle pagine Web e dei relativi oggetti sono trascritte nel registro*. **Shadowing: Incoming Files -** attiva la copia shadow dei file scaricati da un sito Web. *Nel registro vengono scritte le copie shadow dei file scaricati*. **Shadowing: Outgoing Data -** Questo diritto non ha effetti sulla copia shadow. *Nel registro vengono scritte le copie shadow delle richieste HTTP*. **Shadowing: POST Requests -** attiva la copia shadow dei dati immessi nei moduli Web. *Nel registro vengono scritte le copie shadow dei dati immessi nei moduli Web*. **Shadowing: Outgoing Files -** attiva la copia shadow dei file caricati su un sito Web. *Nel registro vengono scritte le copie shadow dei file caricati*.

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
ICQ/AOL Messenger	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi al server di ICQ e AOL Instant Messenger. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro.* **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, gli ID di tutti i partecipanti alla messaggistica immediata, l'indirizzo IP con il numero di porta e il nome dell'host. L'ID del partecipante locale precede quello di un partecipante remoto.* **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti.* **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi inviati.*
IRC	**Audit: Connection -** attiva la registrazione del controllo dei tentativi degli utenti di connettersi a un server IRC. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro.* **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, gli ID di tutti i partecipanti alla messaggistica immediata, l'indirizzo IP con il numero di porta e il nome dell'host. L'ID del partecipante locale precede quello di un partecipante remoto.* **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti.* **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata.*

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
	Contiene una registrazione esatta di tutti i messaggi inviati.
Jabber	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi a un server Jabber. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro.* **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, gli ID di tutti i partecipanti alla messaggistica immediata, l'indirizzo IP con il numero di porta e il nome dell'host. L'ID del partecipante locale precede quello di un partecipante remoto.* **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti.* **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi inviati.*
Mail.ru Agent	**Audit: Connection -** attiva la registrazione del controllo dei tentativi degli utenti di connettere Mail.ru Agent al server Mail.ru. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, gli ID di tutti i partecipanti alla messaggistica immediata, l'indirizzo IP con il numero di porta e il nome dell'host. L'ID del partecipante locale precede quello di un partecipante remoto*. **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti*. **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30*

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
	minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi inviati.
SMTP	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi a un server SMTP. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Outgoing Messages**, **Audit: Outgoing Files** - attiva la registrazione del controllo dei tentativi degli utenti di inviare un messaggio e-mail con o senza allegati. *Nel registro vengono scritti l'azione Outgoing Message, l'indirizzo e-mail del mittente e dei destinatari, l'indirizzo IP con il numero di porta e il nome dell'host. L'indirizzo del mittente precede quello dei destinatari (mittente=>destinatario1, destinatario2)*. **Shadowing: Outgoing Messages**, **Shadowing: Outgoing Files** - attiva la copia shadow dei messaggi e-mail inviati con o senza allegati. *Nel registro vengono scritte le copie shadow dei messaggi e-mail inviati con o senza allegati in formato .eml. I file .eml possono essere aperti, ad esempio, con Microsoft Outlook Express, Windows Mail e Mozilla Thunderbird*.
Social Networks	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi al sito di una rete sociale. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Outgoing Message** - attiva la registrazione del controllo dei tentativi degli utenti di inviare messaggi, commenti, post, ecc. *Nel registro vengono scritte l'azione Outgoing Message e le seguenti informazioni (<nome_sito>_<nome_contenuto>_<ID destinatario>). Gli ID dei destinatari vengono scritti nel registro solo se gli utenti cercano di inviare messaggi. Gli ID dei destinatari vengono scritti in formato numerico*. **Audit: Outgoing Files** - attiva la registrazione del controllo dei tentativi degli utenti di caricare file multimediali e contenuti sul sito di una rete sociale. *Nel registro vengono scritte l'azione Outgoing File e le seguenti informazioni (<nome_sito>_<nome_file>)*. **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi, commenti, post inviati, ecc. *Nel registro vengono scritti le copie shadow dei messaggi inviati, i commenti, ecc*. **Shadowing: Outgoing Files** - attiva la copia shadow dei file caricati sul sito di una rete sociale. *Nel registro vengono scritte le copie shadow dei file caricati*.
Telnet	**Audit: Connection -** attiva la registrazione del controllo dei tentativi degli utenti di connettersi a un sito Telnet. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione*

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
	di un nome di host non funziona, il nome dell'host non viene scritto nel registro.
Web Mail	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di accedere alla Webmail. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Outgoing Messages**, **Audit: Outgoing Files** - attiva la registrazione del controllo dei tentativi degli utenti di inviare un messaggio e-mail con o senza allegati. *Nel registro vengono scritti l'azione Outgoing Message, il nome del provider di posta elettronica (ad esempio Yahoo!, Gmail, Hotmail), l'indirizzo e-mail del mittente e dei destinatari, l'indirizzo IP con il numero di porta e il nome dell'host. L'indirizzo del mittente precede quello dei destinatari (mittente=>destinatario1, destinatario2)*. **Shadowing: Outgoing Messages**, **Shadowing: Outgoing Files** - attiva la copia shadow dei messaggi e-mail inviati con o senza allegati. *Nel registro vengono scritte le copie shadow dei messaggi e-mail inviati con o senza allegati in formato .eml. I file .eml possono essere aperti, ad esempio, con Microsoft Outlook Express, Windows Mail e Mozilla Thunderbird*. **Nota:** i servizi di Webmail salvano automaticamente le bozze dei messaggi. DeviceLock gestisce il salvataggio di una bozza come l'invio di un messaggio.
Windows Messenger	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi al server di Windows Messenger. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, l'ID del partecipante locale, l'indirizzo IP con il numero di porta e il nome dell'host*. **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti*. **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi inviati*.

PROTOCOLLO	DIRITTI DI CONTROLLO/SHADOWING
Yahoo Messenger	**Audit: Connection** - attiva la registrazione del controllo dei tentativi degli utenti di connettersi al server di Yahoo Messenger. *Nel registro vengono scritti l'azione Connection, l'indirizzo IP con il numero di porta e il nome dell'host e il nome del protocollo. Se l'indirizzo IP della risoluzione di un nome di host non funziona, il nome dell'host non viene scritto nel registro*. **Audit: Incoming Messages**, **Outgoing Messages** - attiva la registrazione del controllo dei tentativi degli utenti di inviare e ricevere messaggi immediati. *Nel registro vengono scritti l'azione Chat, gli ID di tutti i partecipanti alla messaggistica immediata, l'indirizzo IP con il numero di porta e il nome dell'host. L'ID del partecipante locale precede quello di un partecipante remoto*. **Shadowing: Incoming Messages** - attiva la copia shadow dei messaggi immediati ricevuti. *Nel registro vengono scritte le copie shadow dei messaggi immediati ricevuti in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi ricevuti*. **Shadowing: Outgoing Messages** - attiva la copia shadow dei messaggi immediati inviati. *Nel registro vengono scritte le copie shadow dei messaggi immediati inviati in formato .txt. Una copia shadow dei messaggi viene scritta nel registro dopo 30 minuti di inattività (vale a dire 30 minuti dopo l'ultimo scambio attivo nella finestra della chat) o quando l'utente abbandona la messaggistica immediata. Contiene una registrazione esatta di tutti i messaggi inviati*.

Nota: è possibile definire diverse regole di controllo e shadowing online od offline per lo stesso utente o gli stessi gruppi di utenti. Le regole di controllo e shadowing online (Regular Profile) si applicano ai computer client che operano online. Le regole di controllo e shadowing offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire le regole di controllo e shadowing offline per i protocolli, consultare la sezione "Gestione delle regole di controllo e shadowing offline per i protocolli".

È possibile definire le regole di controllo e shadowing predefinite per i protocolli per entrambi i tipi di profilo (Regular Profile e Offline Profile). Le regole predefinite si applicano ai gruppi Users ed Everyone. La seguente tabella illustra i diritti concessi a questi gruppi per impostazione predefinita.

GRUPPO / PROTOCOLLO	USERS	EVERYONE
FTP	Audit: Connection Audit: Incoming Files Audit: Outgoing Files	Audit: Connection Audit: Incoming Files Audit: Outgoing Files

GRUPPO / PROTOCOLLO	USERS	EVERYONE
HTTP	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files	Audit: Connection Audit: Incoming Data Audit: Incoming Files Audit: Outgoing Data Audit: POST Requests Audit: Outgoing Files
ICQ/AOL Messenger	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
IRC	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Jabber	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Mail.ru Agent	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
SMTP	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Social Networks	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Telnet	Audit: Connection	Audit: Connection
Web Mail	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files	Audit: Connection Audit: Outgoing Messages Audit: Outgoing Files
Windows Messenger	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages	Audit: Connection Audit: Incoming Messages Audit: Outgoing Messages
Yahoo Messenger	Audit: Connection Audit: Incoming Messages	Audit: Connection Audit: Incoming Messages

GRUPPO / PROTOCOLLO	USERS	EVERYONE
	Audit: Outgoing Messages	Audit: Outgoing Messages

La gestione delle regole di controllo e shadowing online (regolari) per i protocolli include le seguenti attività:

- Definizione e modifica delle regole di controllo e shadowing
- Rimozione della definizione delle regole di controllo e shadowing

Le regole di controllo e shadowing online per un protocollo possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le regole di controllo e shadowing non sono state definite per un protocollo.
Configured	Indica che le regole di controllo e shadowing sono state definite per un protocollo.
No Audit	Indica una delle seguenti condizioni: • I diritti di Audit (Controllo) non sono stati impostati per tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un protocollo. • Tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un protocollo sono stati rimossi. • L'account Everyone non dispone dei diritti Audit e Shadowing ed è l'unico account specificato nelle regole di controllo e shadowing per un protocollo.

Definizione e modifica delle regole di controllo e shadowing

Per definire e modificare le regole di controllo e shadowing

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

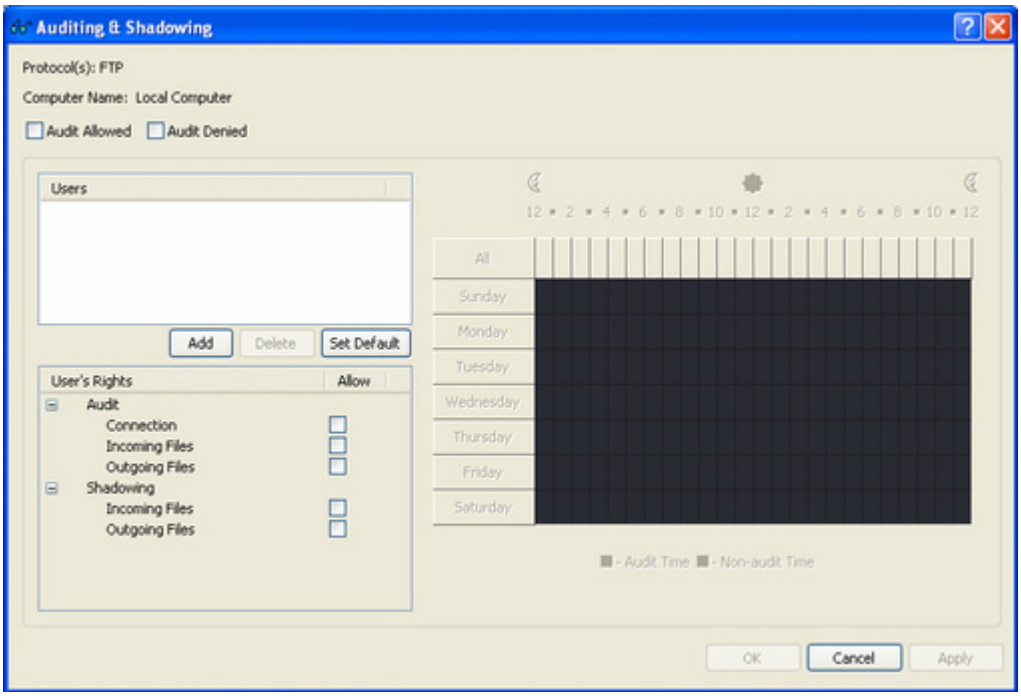
   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Auditing & Shadowing**.

Dopo aver selezionato Auditing & Shadowing nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile definire le regole di controllo e shadowing. Nella colonna Regular del riquadro dei dettagli viene visualizzato lo stato corrente delle regole online per ciascun protocollo.

4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse sul protocollo per cui si desidera definire o modificare le regole, quindi scegliere **Set Auditing & Shadowing**.
     - OPPURE -
   - Selezionare il protocollo per cui si desidera definire o modificare le regole, quindi fare clic su **Set Auditing & Shadowing** sulla barra degli strumenti.
     - OPPURE -
   - Fare doppio clic sul protocollo per cui si desidera definire o modificare le regole.

   Viene visualizzata la finestra di dialogo Auditing & Shadowing.



5. Nella finestra di dialogo **Auditing & Shadowing**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Definire le regole di controllo e shadowing predefinite	1. Nel riquadro superiore sinistro della finestra di dialogo, specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a un protocollo andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a un protocollo non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**.

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
	Le regole di controllo e shadowing predefinite si applicano ai gruppi Users ed Everyone. Per informazioni sui diritti di controllo e shadowing impostati per questi account per impostazione predefinita, consultare la sezione "Gestione delle regole di controllo e shadowing per i protocolli".
Definire le regole di controllo e shadowing per un ulteriore utente o gruppo	1. Nel riquadro superiore sinistro della finestra di dialogo, specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a un protocollo andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a un protocollo non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 3. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Auditing & Shadowing*. 4. Nel riquadro superiore sinistro della finestra di dialogo **Auditing & Shadowing**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi*. 5. Nel riquadro inferiore sinistro della finestra di dialogo **Auditing & Shadowing**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti appropriati. *Nel riquadro destro della finestra di dialogo Auditing & Shadowing, si possono specificare i giorni e le ore (ad esempio dalle 7 alle 17, dal lunedì al venerdì) in cui la regola per l'utente o il gruppo selezionato risulterà attiva o non attiva. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui la regola sarà attiva (orario di controllo). Utilizzare il pulsante destro del mouse per contrassegnare i giorni e le ore in cui la regola non sarà attiva (orario senza controllo)*.
Modificare le regole di controllo e shadowing per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti appropriati.

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Rimuovere un utente o gruppo esistente e le regole associate	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC. *Quando viene rimosso un utente o un gruppo, vengono rimosse anche tutte le regole associate a tale utente o gruppo*.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle regole di controllo e shadowing

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che le regole di controllo e shadowing definite per uno o più protocolli specifici vengano applicate a un determinato gruppo di computer client. Per farlo, occorre reimpostare lo stato non configurato per le regole precedentemente definite. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Per rimuovere la definizione delle regole di controllo e shadowing

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
   c) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile definire le regole di controllo e shadowing.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere la definizione delle regole, quindi scegliere **Undefine**.

   È possibile rimuovere simultaneamente la definizione delle regole per più protocolli. Per farlo, attenersi alle seguenti istruzioni:
   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui protocolli.

b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine**.

Gestione della lista bianca dei protocolli

La lista bianca dei protocolli consente di autorizzare in maniera selettiva le comunicazioni di rete su tutti i protocolli supportati, indipendentemente dalle impostazioni di blocco dei protocolli esistenti. Questa funzione è particolarmente utile nelle situazioni in cui si dispone di pochi privilegi e in cui viene bloccato tutto il traffico dei protocolli e, in seguito, vengono autorizzati solo i protocolli necessari per l'esecuzione delle normali attività lavorative da parte dei dipendenti.

Ad esempio, è possibile negare a tutti gli utenti l'accesso ai protocolli SMTP e Web Mail e, in seguito, utilizzare la lista bianca per autorizzare determinati utenti a inviare e-mail a indirizzi e-mail specifici, consentendo a tali utenti di svolgere le proprie attività lavorative. Applicando criteri di protezione del genere, è possibile ridurre al minimo i rischi di perdita, furto e utilizzo improprio dei dati.

Nota: il controllo e la copia shadow non vengono eseguiti per i trasferimenti di dati autorizzati dalla lista bianca dei protocolli, mentre le connessioni autorizzate vengono controllate.

La lista bianca contiene le regole associate al protocollo specificato. Ciascuna regola specifica gli utenti o i gruppi cui viene applicata e contiene una serie di parametri. Tali parametri rientrano in due categorie:

- Parametri generali che si applicano a tutti i protocolli
- Parametri specifici per protocollo.

La seguente tabella descrive i parametri generali per una regola della lista bianca.

PARAMETRO	DESCRIZIONE
Protocol	Specifica il protocollo cui si applica la regola.
Description	Specifica il nome della regola.

La seguente tabella descrive i parametri specifici per protocollo per una regola della lista bianca.

PARAMETRO	DESCRIZIONE
Hosts:	Si applica ai protocolli FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, Telnet, Windows Messenger e Yahoo Messenger. Specifica una lista di host autorizzati per questa regola. Se viene specificata la lista, questi host non vengono bloccati. Gli host possono essere specificati in uno qualsiasi dei seguenti formati: • Nome di DNS (ad esempio **www.esempio.com**). È possibile utilizzare il carattere jolly dell'asterisco (*) nei nomi di DNS (ad esempio

PARAMETRO	DESCRIZIONE
	***.esempio.com** indica che il nome di host equivale a qualsiasi server il cui nome termina con il termine specificato). **Avviso:** l'aggiunta nella lista bianca di nomi di host con caratteri jolly per tutti i protocolli (tranne HTTP) non garantisce il funzionamento previsto della regola della lista bianca. Poiché DeviceLock utilizza il file degli host locale per la risoluzione del nome dell'host, un utente malintenzionato con diritti di amministratore può modificare il file degli host per da superare i criteri di protezione di DeviceLock. Se, ad esempio, la lista bianca autorizza l'accesso in HTTP a gmail.com, un utente malintenzionato con diritti di amministratore può accedere all'elemento www.ru non autorizzato aggiungendo la voce "**194.87.0.50 gmail.com**" al file degli host. Per ridurre al minimo di rischi di sicurezza, si consiglia di specificare gli indirizzi IP al posto dei nomi di host. • Indirizzo IP (ad esempio **12.13.14.15**). È possibile specificare un intervallo di indirizzi IP separati da un trattino (-) (ad esempio **12.13.14.18-12.13.14.28**). È inoltre possibile specificare la subnet mask per l'indirizzo IP utilizzando il seguente formato: *indirizzo IP/dimensione della subnet mask in bit* (ad esempio **3.4.5.6/16**). Gli host multipli vanno separati da una virgola (,) o da un punto e virgola (;). È inoltre possibile premere INVIO dopo ogni voce. È possibile specificare più host nei diversi formati sopracitati (ad esempio www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28). **Nota:** durante l'aggiunta di host alla lista bianca, considerare quanto segue: Se gli oggetti di una pagina Web (immagini, script, filmati, file Flash, ActiveX, ecc.) vengono scaricati da altri host, è necessario aggiungere questi ultimi alla lista bianca per caricare la pagina Web correttamente. Se vengono specificati gli host ma non le porte, è possibile accedere agli host attraverso tutte le porte disponibili. Un'applicazione dotata di un certificato SSL incorporato (ad esempio Microsoft Office Communicator, Dropbox, iTunes, modulo di sincronizzazione dei contatti di Google, ecc.) non riuscirà a connettersi al proprio server mentre è attivo il modulo di NetworkLock. Il modulo di NetworkLock diventa attivo quando vengono definite le impostazioni per i protocolli. Per risolvere questo problema, aggiungere l'host del server alla lista bianca di SSL. È possibile utilizzare TcpView per consultare il contenuto dell'host del server. Aggiungendo un host del server alla lista bianca, tutto il traffico SSL tra un'applicazione e l'host del server specificato supera il controllo dell'accesso, la verifica, la copia shadow e il filtraggio del contenuto.
Ports:	Si applica ai protocolli FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, Telnet, Windows Messenger e Yahoo Messenger. Specifica la porta o le porte da aprire per questa regola. Se viene specificata la lista, queste porte non vengono bloccate. È possibile specificare un'unica porta o un intervallo inclusivo di porte separate da

PARAMETRO	DESCRIZIONE
	un trattino (-). Ad esempio, per aprire la porta 25, immettere **25**. Per aprire le porte da 5000 a 5020 (incluse), immettere **5000-5020**. Le porte multiple o gli intervalli di porte vanno separati da una virgola (,) o da un punto e virgola (;). Ad esempio **25, 36; 8080, 5000-5020**. È inoltre possibile premere INVIO dopo ogni voce. **Nota:** se vengono specificate le porte ma non gli host, gli utenti possono accedere a tutti gli host disponibili tramite le porte specificate.
SSL	Si applica ai protocolli FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, SMTP e Web Mail. Consente di impostare le opzioni SSL. Sono disponibili le seguenti opzioni SSL: • **Allowed** autorizza le connessioni SSL. • **Denied** nega le connessioni SSL. • **Required** richiede l'utilizzo di SSL da parte di tutte le connessioni.
Local sender ID(s):	Si applica ai protocolli ICQ/AOL Messenger, Jabber, Mail.ru Agent, Windows Messenger e Yahoo Messenger. Specifica una lista di ID di utenti locali autorizzati a inviare messaggi immediati. Se viene specificata questa lista, i messaggi immediati provenienti da tali utenti non verranno bloccati. Gli utenti di ICQ/AOL Messenger vengono identificati da numeri noti come UIN (ad esempio **111222, 23232323**). Gli utenti di Jabber vengono identificati dagli ID di Jabber nel seguente formato: **utente@esempio.com**. Gli utenti di Mail.ru Agent vengono identificati indirizzi e-mail di mail.ru nel seguente formato: **utente@mail.ru**. Gli utenti di Windows Messenger vengono identificati dagli indirizzi e-mail nel seguente formato: **utente@esempio.com**. Gli utenti di Yahoo Messenger vengono identificati da uno dei seguenti ID utente: • **Yahoo! ID** (<nome utente> o <nome utente>@yahoo.com) • **Rocketmail** (<nome utente>@rocketmail.com) • **Ymail** (<nome utente>@ymail.com) Gli ID utente multipli vanno separati da una virgola (,) o da un punto e virgola (;). È inoltre possibile premere INVIO dopo ogni voce.
Remote recipient ID(s):	Si applica ai protocolli ICQ/AOL Messenger, Jabber, Mail.ru Agent e Yahoo Messenger. Specifica una lista di ID di utenti remoti autorizzati a ricevere messaggi immediati. Se viene specificata questa lista, i messaggi immediati inviati a tali utenti non verranno bloccati. Gli utenti di ICQ/AOL Messenger vengono identificati da numeri noti come UIN (ad esempio **111222, 23232323**). Gli utenti di Jabber vengono identificati dagli ID di Jabber nel seguente formato: **utente@esempio.com**. Gli utenti di Mail.ru Agent vengono identificati indirizzi e-mail di mail.ru nel

PARAMETRO	DESCRIZIONE
	seguente formato: **utente@mail.ru**. Gli utenti di Windows Messenger vengono identificati dagli indirizzi e-mail nel seguente formato: **utente@esempio.com**. Gli utenti di Yahoo Messenger vengono identificati da uno dei seguenti ID utente: • **Yahoo! ID** (<nome utente> o <nome utente>@yahoo.com) • **Rocketmail** (<nome utente>@rocketmail.com) • **Ymail** (<nome utente>@ymail.com) Gli ID utente multipli vanno separati da una virgola (,) o da un punto e virgola (;). È inoltre possibile premere INVIO dopo ogni voce.
Local sender Email(s):	Si applica ai protocolli SMTP e Web Mail. Specifica una lista di mittenti di e-mail autorizzati per questa regola. Se viene specificata questa lista, i messaggi e-mail provenienti da tali mittenti non verranno bloccati. Immettere gli indirizzi dei mittenti nel seguente formato: *utente@dominio.com*. È possibile utilizzare l'asterisco (*) come carattere jolly per specificare un gruppo di mittenti. È possibile aggiungere l'asterisco prima o dopo il simbolo della chiocciola (@) in un indirizzo e-mail. Ad esempio, per autorizzare la ricezione di e-mail da tutti gli utenti di un dominio, digitare ***@dominio.com**. Gli indirizzi e-mail multipli vanno separati da una virgola (,) o da un punto e virgola (;). È inoltre possibile premere INVIO dopo ogni voce. **Nota:** durante l'aggiunta di mittenti/destinatari alla lista bianca di Webmail, considerare quanto segue: i messaggi inviati da un'applicazione Webmail vengono memorizzati nella cartella della posta inviata e possono essere inoltrati a qualunque indirizzo da qualsiasi computer.
Remote recipient Email(s):	Si applica ai protocolli SMTP e Web Mail. Specifica una lista di destinatari di e-mail autorizzati per questa regola. Se viene specificata questa lista, i messaggi e-mail inviati a questi destinatari non verranno bloccati. Immettere gli indirizzi dei destinatari nel seguente formato: *utente@dominio.com*. È possibile utilizzare l'asterisco (*) come carattere jolly per specificare un gruppo di mittenti. È possibile aggiungere l'asterisco prima o dopo il simbolo della chiocciola (@) in un indirizzo e-mail. Ad esempio, per autorizzare l'invio di e-mail a tutti gli utenti di un dominio, digitare ***@dominio.com**. Gli indirizzi e-mail multipli vanno separati da una virgola (,) o da un punto e virgola (;). È inoltre possibile premere INVIO dopo ogni voce.
Social Networks	Si applica al protocollo Social Networks. Specifica una lista di siti di reti sociali autorizzati per questa regola. Se viene specificata la lista, questi siti di reti sociali non vengono bloccati. Sono supportati i seguenti siti di reti sociali: Facebook, Google+, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, SchuelerVZ, StudiVZ, Tumblr, Twitter, Vkontakte, XING.
Web Mail Services	Si applica al protocollo Web Mail. Specifica una lista di servizi di e-mail basati sul Web per questa regola. Se viene specificata la lista, i messaggi e-mail inviati tramite questi servizi di Webmail non verranno bloccati. Sono supportati i seguenti servizi e-mail basati sul Web: AOL Mail, Gmail, GMX Mail, Hotmail, Mail.ru,

PARAMETRO	DESCRIZIONE
	Rambler Mail, Web.de, Yahoo! Mail, e Yandex Mail.

Nota: è possibile definire più liste bianche dei protocolli online od offline per lo stesso utente o gli stessi gruppi di utenti. La lista bianca dei protocolli online (Regular Profile) si applica ai computer client che operano online. La lista bianca dei protocolli offline (Offline Profile) si applica ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come definire la lista bianca dei protocolli offline, consultare la sezione "Gestione della lista bianca dei protocolli offline".

La gestione della lista bianca dei protocolli online (regolare) include le seguenti attività:

- Definizione della lista bianca dei protocolli
- Modifica della lista bianca dei protocolli
- Copia delle regole della lista bianca dei protocolli
- Esportazione e importazione della lista bianca dei protocolli
- Rimozione della definizione della lista bianca dei protocolli
- Eliminazione delle regole della lista bianca dei protocolli

Definizione della lista bianca dei protocolli

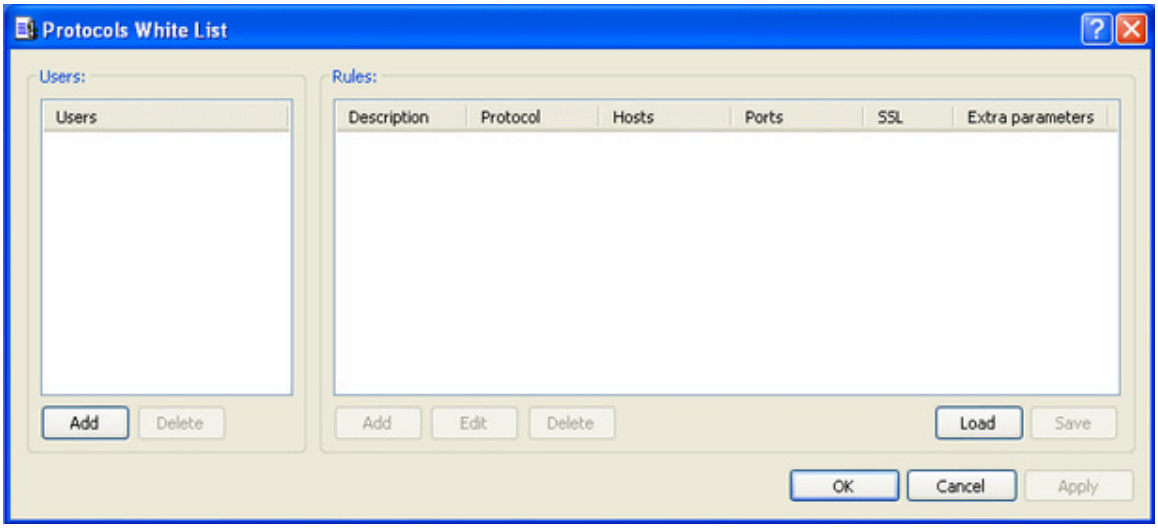
Per definire la lista bianca dei protocolli

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Protocols White List.



4. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la lista bianca dei protocolli, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro sinistro della finestra di dialogo Protocols White List.

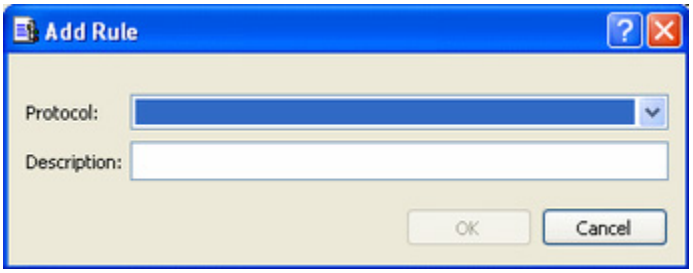
   Per eliminare un utente o un gruppo, nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** .

6. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare l'utente o il gruppo desiderato.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi.

7. Nel riquadro destra della finestra di dialogo **Protocols White List**, sotto **Rules**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, specificare i parametri generali e specifici per protocollo relativi a questa regola. Per specificare i parametri generali, attenersi alle seguenti istruzioni:

- Per specificare il protocollo, selezionarlo nell'elenco **Protocol:**.
- Per specificare il nome della regola, digitarlo nella casella **Description**.

Per specificare i parametri specifici per protocollo, attenersi alle seguenti istruzioni:

- Per specificare gli host, digitare i nomi di host o gli indirizzi IP separati da una virgola o da un punto e virgola nella casella **Hosts:**. Per ulteriori informazioni su come specificare gli host, consultare la descrizione del parametro Hosts illustrata in precedenza in questa sezione.
- Per specificare le porte, digitare i numeri di porta separati da una virgola o da un punto e virgola nella casella **Ports:**. Per ulteriori informazioni su come specificare le porte, consultare la descrizione del parametro Ports illustrata in precedenza in questa sezione.
- Per configurare le opzioni SSL, sotto **SSL**, fare clic su una delle seguenti opzioni: **Allowed** (autorizza le connessioni SSL), **Denied** (nega le connessioni SSL) o **Required** (richiede l'utilizzo di SSL da parte di tutte le connessioni).
- Per specificare gli ID dei mittenti locali di messaggistica immediata, digitare gli ID utente separati da una virgola o da un punto e virgola nella casella **Local sender ID(s):**. Per ulteriori informazioni su come specificare gli ID utente, consultare la descrizione del parametro Local sender ID(s) illustrata in precedenza in questa sezione.
- Per specificare gli ID dei destinatari locali di messaggistica immediata, digitare gli ID utente separati da una virgola o da un punto e virgola nella casella **Remote recipient ID(s):**. Per ulteriori informazioni su come specificare gli ID utente, consultare la descrizione del parametro Remote recipient ID(s) illustrata in precedenza in questa sezione.
- Per specificare i mittenti di e-mail, digitare gli indirizzi dei mittenti separati da una virgola o da un punto e virgola nella casella **Local sender Email(s):**. Per ulteriori informazioni su come specificare gli indirizzi dei mittenti, consultare la descrizione del parametro Local sender Email(s): illustrata in precedenza in questa sezione.
- Per specificare i destinatari di e-mail, digitare gli indirizzi dei destinatari separati da una virgola o da un punto e virgola nella casella **Remote recipient Email(s):**. Per ulteriori informazioni su come specificare gli indirizzi dei destinatari, consultare la descrizione del parametro Remote recipient Email(s): illustrata in precedenza in questa sezione.
- Per specificare i siti delle reti sociali, sotto **Social Networks:** selezionare le caselle di controllo desiderate. Per ulteriori informazioni, consultare la descrizione del parametro Social Networks: illustrata in precedenza in questa sezione.
- Per specificare i servizi e-mail basati sul Web, sotto **Web Mail Services:** selezionare le caselle di controllo desiderate. Per ulteriori informazioni, consultare la descrizione del parametro Web Mail Services: illustrata in precedenza in questa sezione.

9. Fare clic su **OK**.

   La regola creata viene visualizzata sotto Rules nel riquadro destro della finestra di dialogo Protocols White List.

10. Fare clic su **OK** o su **Apply**.

Gli utenti o i gruppi cui si applica una regola della lista bianca vengono visualizzati sotto White List nella struttura della console.

Se nella struttura della console viene selezionato un utente o un gruppo cui si applica una regola della lista bianca, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:

- **Protocol** - Il protocollo cui si applica la regola.
- **Description** - Il nome della regola.
- **Hosts** - Mostra gli host autorizzati per questa regola.
- **Ports** - Mostra le porte autorizzate per questa regola.
- **SSL** - Mostra l'opzione SSL selezionata. Valori possibili: **Allowed** (autorizza le connessioni SSL), **Denied** (nega le connessioni SSL) e **Required** (richiede l'utilizzo di SSL da parte di tutte le connessioni).
- **Extra parameters** - Mostra i parametri extra specifici per protocollo specificati per la regola. I parametri extra sono i seguenti: **From** (mostra gli ID dei mittenti autorizzati per la messaggistica immediata e gli indirizzi e-mail dei mittenti autorizzati per la Webmail) e **To** (mostra gli ID dei destinatari autorizzati per la messaggistica immediata e gli indirizzi dei destinatari autorizzati per la Webmail).
- **Profile** - Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

  È possibile definire più liste bianche dei protocolli online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire la lista bianca dei protocolli offline, consultare la sezione "Gestione della lista bianca dei protocolli offline".

Modifica della lista bianca dei protocolli

È possibile modificare i valori dei parametri specificati per una regola della lista bianca in qualsiasi momento.

Per modificare una regola della lista bianca

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **White List**, scegliere **Manage**, quindi attenersi alla procedura seguente:

a) Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

b) Nel riquadro destro della finestra di dialogo **Protocols White List**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.

- OPPURE -

Fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Edit**.

- OPPURE -

Sotto **Protocols**, espandere **White List**, quindi attenersi alla procedura seguente:

a) Sotto **White List**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi nel riquadro dei dettagli.

b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.

- OPPURE -

Nel riquadro dei dettagli, fare doppio clic sulla regola che si desidera modificare.

Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare i parametri della regola secondo le proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole della lista bianca dei protocolli

Per riutilizzare le regole esistenti della lista bianca dei protocolli, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Per copiare una regola della lista bianca

1. Se si utilizza DeviceLock Management Console:

a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.

b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.

3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Manage** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Protocols White List.
4. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare l'utente o il gruppo cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi sotto Rules, nel riquadro inferiore destro della finestra di dialogo.
5. Nel riquadro destro della finestra di dialogo **Protocols White List**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. Se si usa la combinazione di tasti CTRL+X, la regola viene eliminata solo dopo essere stata incollata.
6. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.
7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro sinistro della finestra di dialogo Protocols White List.
8. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare gli utenti o i gruppi cui applicare la regola copiata.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi.
9. Nel riquadro destro della finestra di dialogo **Protocols White List**, fare clic con il pulsante destro del mouse nel riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro destro della finestra di dialogo Protocols White List.
10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione della lista bianca dei protocolli

È possibile esportare tutte le regole correnti della lista bianca dei protocolli in un file .pwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Per esportare la lista bianca dei protocolli

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Save**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Save** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola della lista bianca, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **White List**, selezionare qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage**. Nel riquadro destro della finestra di dialogo **Protocols White List**, sotto **Rules**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .pwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   La lista bianca dei protocolli esportata viene salvata in un file con estensione .pwl.

Per importare la lista bianca dei protocolli

1. Se si utilizza DeviceLock Management Console:

a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

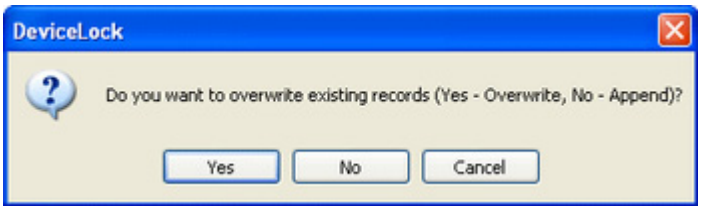
Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Load**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Load** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load**.
     - OPPURE -
   - Espandere **White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola della lista bianca, quindi scegliere **Load**.
     - OPPURE -
   - Espandere **White List**, selezionare qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage**. Nel riquadro destro della finestra di dialogo **Protocols White List**, sotto **Rules**, fare clic su **Load**.

   Viene visualizzata la finestra di dialogo Open.
4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   Se la lista bianca dei protocolli è già definita e si sceglie di importarne una nuova, viene visualizzato il seguente messaggio.



Nella finestra di messaggio, fare clic su **Yes** per sovrascrivere la lista bianca esistente. Fare clic su **No** per aggiungere la nuova lista bianca a quella esistente.

Rimozione della definizione della lista bianca dei protocolli

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che la lista bianca dei protocolli venga applicata a un gruppo specifico di computer client. Per farlo, occorre reimpostare lo stato non configurato per la lista bianca precedentemente definita. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Per rimuovere la definizione della lista bianca dei protocolli

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
   c) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Undefine**.

Eliminazione delle regole della lista bianca dei protocolli

Se alcune regole della lista bianca non sono più necessarie, possono essere eliminate.

Per eliminare una regola della lista bianca

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Espandere **White List**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo cui viene applicata la regola, quindi scegliere **Delete user**.
     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.

     - OPPURE -
   - Espandere **White List** e selezionare l'utente o il gruppo cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage**. Nel riquadro sinistro della finestra di dialogo **Protocols White List**, sotto **Users**, selezionare l'utente o il gruppo cui viene applicata la regola. Nel riquadro destro della finestra di dialogo **Protocols White List**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.

Gestione delle impostazioni di protezione per i protocolli

È possibile definire parametri di protezione aggiuntivi che influiscono sulle autorizzazioni e le regole di controllo per i protocolli.

DeviceLock supporta i seguenti parametri di protezione aggiuntivi:

- **Block unrecognized outgoing SSL traffic**: se questo parametro viene attivato, DeviceLock Service è autorizzato a controllare e bloccare tutto il traffico SSL in uscita non riconosciuto. In caso contrario, anche se i protocolli sono bloccati, tutto il traffico SSL in uscita non riconosciuto non viene bloccato né controllato.
- **Block IP addresses in URL**: se questo parametro viene autorizzato, DeviceLock Service è autorizzato a bloccare tutti gli URL contenenti l'indirizzo IP host se gli utenti dispongono delle autorizzazioni “allow access” per un protocollo. Utilizzare questa impostazione per bloccare l'accesso ai siti (ad esempio Facebook) a cui è possibile accedere utilizzando un indirizzo IP. Questa impostazione si applica ai seguenti protocolli: HTTP, Social Networks e Web Mail. L'opzione è disattivata per impostazione predefinita.
  Il controllo e la copia shadow per gli URL contenenti l'indirizzo IP host vengono eseguiti a livello di HTTP. Se l'opzione Block IP addresses in URL è disattivata, ma gli

utenti dispongono delle autorizzazioni "deny access" per un protocollo, tutti gli URL contenenti l'indirizzo IP host vengono anch'essi bloccati.

Nota: se l'opzione **Block IP addresses in URL** è attivata e alcuni indirizzi IP host specifici sono autorizzati nella lista bianca dei protocolli, tali indirizzi IP non saranno bloccati. Le impostazioni della lista bianca dei protocolli hanno la precedenza sulle impostazioni di protezione dei protocolli.

Nota: è possibile definire diverse impostazioni di protezione online od offline per lo stesso utente o gli stessi gruppi di utenti. Le impostazioni di protezione online (Regular Profile) si applicano ai computer client che operano online. Le impostazioni di protezione offline (Offline Profile) si applicano ai computer client che operano offline. Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client. Per informazioni dettagliate sui criteri offline di DeviceLock, consultare la sezione "Criteri di protezione DeviceLock (Offline Profile)". Per informazioni su come impostare le impostazioni di protezione offline, consultare la sezione "Gestione delle impostazioni di protezione offline per i protocolli".

La gestione delle impostazioni di protezione (regolari) per i protocolli include le seguenti attività:

- Definizione e modifica delle impostazioni di protezione
- Rimozione della definizione delle impostazioni di protezione

Le impostazioni di protezione per i protocolli possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le impostazioni di protezione non sono definite per i protocolli.
Enabled	Indica che le impostazioni di protezione sono definite per i protocolli.
Disabled	Indica che le impostazioni di protezione sono disattivate per i protocolli.

Definizione e modifica delle impostazioni di protezione

Per definire e modificare le impostazioni di protezione

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Selezionare **Security Settings**. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sull'impostazione di protezione, quindi scegliere **Enable** o **Disable**.

     Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

     - OPPURE-
   - Fare clic con il pulsante destro del mouse su **Security Settings**, quindi scegliere **Manage**. Nella finestra di dialogo **Security Settings** visualizzata, selezionare o deselezionare le caselle di controllo pertinenti e fare clic su **OK**.

     La finestra di dialogo Security Settings può essere inoltre aperta selezionando Security Settings e, in seguito, facendo clic su Manage sulla barra degli strumenti.

Rimozione della definizione delle impostazioni di protezione

Se i criteri di DeviceLock vengono implementati tramite DeviceLock Group Policy Manager o DeviceLock Service Settings Editor, in alcune situazioni può risultare utile evitare che le impostazioni di protezione definite per i protocolli vengano applicate a un gruppo specifico di computer client. Per farlo, occorre reimpostare lo stato non configurato per le impostazioni di protezione precedentemente definite. Tutte le impostazioni di DeviceLock non definite vengono ignorate dai computer client.

Per rimuovere la definizione delle impostazioni di protezione

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
   c) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Security Settings**.

   Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sull'impostazione di protezione per cui si desidera rimuovere la definizione, quindi scegliere **Undefine**.

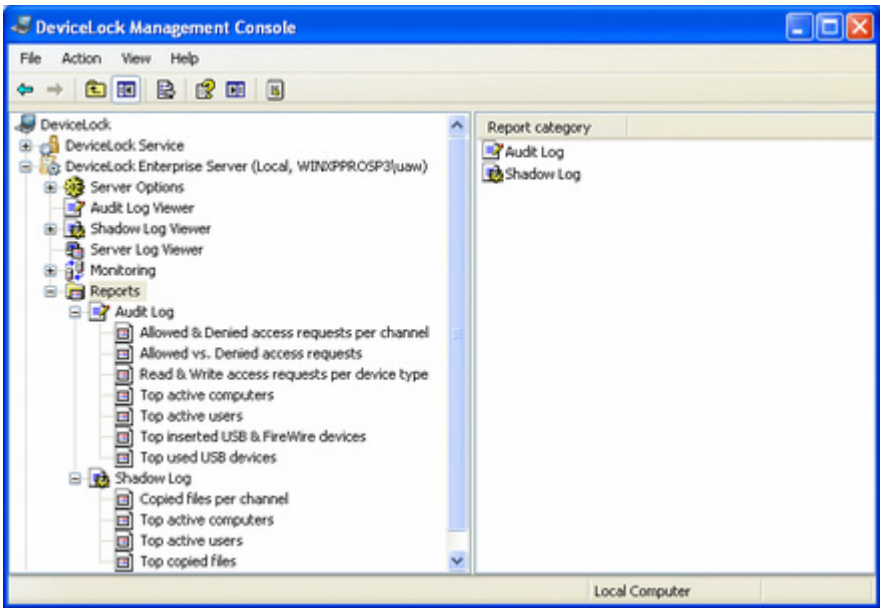
Rapporti di DeviceLock

DeviceLock consente di creare rapporti ricorrendo ai dati dei registri memorizzati su DeviceLock Enterprise Server. È possibile utilizzare i rapporti per classificare e visualizzare dati statistici sulle attività di un utente relative a periferiche e protocolli in un file separato. Durante la generazione di un rapporto, è possibile definirne i parametri per filtrare i dati e visualizzare le informazioni desiderate. Ad esempio, si possono specificare la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati.

I rapporti possono essere creati, inviati automaticamente all'utente tramite e-mail, memorizzati, esportati in diversi formati e condivisi con altri utenti. I rapporti vengono creati tramite DeviceLock Management Console.

Categorie e tipi di rapporti

DeviceLock include una serie di modelli di rapporto predefiniti, che possono essere utilizzati per creare nuovi rapporti. I modelli predefiniti sono visualizzati nella struttura della console, sotto **DeviceLock Enterprise Server**, **Reports**.



Nota: è possibile creare solo rapporti basati sui modelli predefiniti. Non è possibile modificare i modelli di rapporto predefiniti né creare modelli di rapporti personalizzati.

Sono disponibili due categorie di modelli di rapporto:

- Rapporti Audit Log
- Rapporti Shadow Log

Di seguito vengono descritti i tipi di rapporto disponibili in ciascuna categoria.

Nota: se viene effettuato l'aggiornamento alla versione 7.0 di DeviceLock, i rapporti precedentemente generati vengono automaticamente aggiornati con il nuovo nome. Il nome dei rapporti "Allowed & Denied access requests per device type" cambia in "Allowed & Denied access requests per channel". Il nome dei rapporti "Allowed vs. Denied device access" cambia in "Allowed vs. Denied access requests". Il nome dei rapporti "Copied files per device type" cambia in "Copied files per channel".

Rapporti Audit Log

I rapporti Audit Log utilizzano i file di registro di controllo di DeviceLock Enterprise Server come origine dati. La seguente tabella fornisce informazioni di riepilogo dei tipi di rapporto disponibili in questa categoria.

TIPO DI RAPPORTO	DESCRIZIONE
Allowed & Denied access requests per channel	Questo rapporto indica la quantità di richieste di accesso approvate e negate per canale di trasmissione dati (periferiche e/o protocolli). Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **User(s):** mostra gli utenti specificati per il rapporto. • **Channel(s):** mostra i canali di trasmissione dati specificati per il rapporto. Le opzioni disponibili sono: **all devices**, **all protocols** e **all devices and protocols**. La sezione Risultati rapporto include una tabella e un grafico che mostrano risultati dettagliati del rapporto. La tabella presenta le seguenti colonne: • **Channel** mostra un canale di trasmissione dati. • **Allowed** mostra il numero di richieste di accesso approvate. • **Denied** mostra il numero di richieste di accesso negate.
Allowed vs. Denied access requests	Questo rapporto indica il totale delle richieste di accesso approvate e negate, inviate attraverso tutti i canali di trasmissione dati (periferiche e/o protocolli). Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati.

TIPO DI RAPPORTO	DESCRIZIONE
	Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server. • **Computer(s):** mostra i computer specificati per il rapporto. • **User(s):** mostra gli utenti specificati per il rapporto. • **Channel(s):** mostra i canali di trasmissione dati specificati per il rapporto. Le opzioni disponibili sono: **all devices**, **all protocols** e **all devices and protocols**. La sezione Risultati rapporto include una tabella e un diagramma che mostrano risultati dettagliati del rapporto. La tabella presenta le seguenti righe: • **Allowed** mostra il numero totale di richieste di accesso approvate e la relativa percentuale. • **Denied** mostra il numero totale di richieste di accesso negate e la relativa percentuale. • **Total** mostra il numero totale di richieste di accesso e la relativa percentuale. Il diagramma mostra i risultati del rapporto in termini percentuali.
Read & Write access requests per device type	Questo rapporto indica il numero di richieste di accesso di lettura e scrittura per tipo di periferica. Il rapporto fornisce dati solo per i seguenti tipi di periferica: floppy, iPhone, rimovibile, DVD/CD-ROM, nastro, Windows Mobile e Palm. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Access Type(s):** mostra i tipi di evento specificati per il rapporto. • **Computer(s):** mostra i computer specificati per il rapporto. • **User(s):** mostra gli utenti specificati per il rapporto. La sezione Risultati rapporto include una tabella e un grafico che mostrano risultati dettagliati del rapporto. La tabella presenta le seguenti colonne: • **Device Type** mostra il tipo di periferica. • **Read** mostra il numero di richieste di accesso di lettura. • **Write** mostra il numero di richieste di accesso di scrittura. La tabella presenta anche una riga **Total** che specifica la somma di tutti i valori delle colonne **Read** e **Write**.
Top active computers	Questo rapporto mostra i computer utilizzati con più frequenza, classificati in base al numero di richieste di accesso approvate e negate. Per impostazione predefinita, il rapporto include i primi 10 computer, ma è possibile specificare un numero qualsiasi.

TIPO DI RAPPORTO	DESCRIZIONE
	Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Channel(s):** mostra i tipi di periferica e/o i protocolli specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene i principali N (in cui N è un numero specifico) computer per cui l'accesso è autorizzato. La tabella n° 2 contiene i principali N (in cui N è un numero specifico) computer per cui l'accesso è negato. Queste tabelle presentano le seguenti colonne: • **Computer Name** mostra il nome del computer • **Access Count** mostra il numero di richieste di accesso. I valori di questa colonna sono classificati in ordine discendente.
Top active users	Questo rapporto mostra gli utenti più attivi, classificati in base al numero di richieste di accesso approvate e negate inviate da ciascun utente. Per impostazione predefinita, il rapporto include i primi 10 utenti, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **Channel(s):** mostra i tipi di periferica e/o i protocolli specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene i principali N (in cui N è un numero specifico) utenti per cui l'accesso è autorizzato. La tabella n° 2 contiene i principali N (in cui N è un numero specifico) utenti per cui l'accesso è negato. Queste tabelle presentano le seguenti colonne: • **User Name** mostra il nome dell'utente • **Access Count** mostra il numero di richieste di accesso. I valori di questa

TIPO DI RAPPORTO	DESCRIZIONE
	colonna sono classificati in ordine discendente.
Top inserted USB & FireWire devices	Questo rapporto mostra le periferiche USB e FireWire inserite con più frequenza, classificate in base al numero di azioni Insert. Per impostazione predefinita, il rapporto include le prime 10 periferiche, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **Users(s):** mostra gli utenti specificati per il rapporto. La sezione Risultati rapporto include una tabella con i risultati dettagliati del rapporto. Questa tabella presenta le seguenti colonne: • **Device Name** mostra il nome della periferica. • **Insert Count** nostra il numero di azioni Insert. I valori di questa colonna sono classificati in ordine discendente.
Top used USB devices	Questo rapporto mostra le periferiche USB utilizzate con più frequenza, classificate in base al numero di richieste di accesso approvate e negate. Per impostazione predefinita, il rapporto include le prime 10 periferiche, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **Users(s):** mostra gli utenti specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene le principali N (in cui N è un numero specifico) periferiche USB per cui l'accesso è autorizzato. La tabella n° 2 contiene le principali N (in cui N è un numero specifico) periferiche USB per cui l'accesso è negato. Queste tabelle presentano le seguenti colonne:

TIPO DI RAPPORTO	DESCRIZIONE
	• **Device Name** mostra il nome della periferica. • **Access Count** mostra il numero di richieste di accesso. I valori di questa colonna sono classificati in ordine discendente.

Rapporti Shadow Log

I rapporti Shadow Log utilizzano i file di registro shadowing di DeviceLock Enterprise Server come origine dati. Tutti i rapporti includono i dati combinati provenienti dal registro shadowing e dal registro shadowing eliminato. La seguente tabella fornisce informazioni di riepilogo dei tipi di rapporto disponibili in questa categoria.

TIPO DI RAPPORTO	DESCRIZIONE
Copied files per channel	Questo rapporto mostra i dati statistici sui dati copiati per canale di trasmissione dati (periferiche e/o protocolli). I dati statistici sui file copiati vengono classificati in base al numero di file copiati e alla dimensione totale di tutti i file copiati. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **Users(s):** mostra gli utenti specificati per il rapporto. • **File Name:** mostra i file specificati per il rapporto. • **Channel(s):** mostra i canali di trasmissione dati specificati per il rapporto. Le opzioni disponibili sono: **all devices**, **all protocols** e **all devices and protocols**. La sezione Risultati rapporto include due tabelle e due diagrammi che mostrano i risultati dettagliati del rapporto. La tabella n° 1 indica il numero di file copiati per ciascun canale di trasmissione dati. La tabella n° 1 presenta la seguenti colonne: • **Channel** mostra un canale di trasmissione dati. • **Number of Files** mostra il numero di file copiati. La tabella n° 1 presenta anche una riga **Total** che specifica la somma di tutti i valori della colonna **Number of Files**. La tabella n° 2 mostra la dimensione totale dei file copiati per ciascun canale di trasmissione dati. La tabella n° 2 presenta la seguenti colonne: • **Channel** mostra un canale di trasmissione dati. • **Data Size** mostra la dimensione totale di tutti i file copiati.

TIPO DI RAPPORTO	DESCRIZIONE
	La tabella n° 2 presenta anche una riga **Total** che specifica la somma di tutti i valori della colonna **Data Size**. Ciascuna tabella è corredata da un diagramma che rappresenta i risultati del rapporto in termini percentuali.
Top active computers	Questo rapporto mostra i computer utilizzati con più frequenza, classificati in base al numero di file copiati e alla dimensione totale di tutti i file copiati. Per impostazione predefinita, il rapporto include i primi 10 computer, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Channel(s):** mostra i tipi di periferica e/o i protocolli specificati per il rapporto. • **File Name:** mostra i file specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene i principali N (in cui N è un numero specifico) computer per numero di file copiati. La tabella n° 1 presenta la seguenti colonne: • **Computer Name** mostra il nome del computer. • **Number of Files** mostra il numero di file copiati. I valori di questa colonna sono classificati in ordine discendente. La tabella n° 2 contiene i principali N (in cui N è un numero specifico) computer per quantità di dati copiati. La tabella n° 2 presenta la seguenti colonne: • **Computer Name** mostra il nome del computer. • **Data Size** mostra la dimensione totale di tutti i file copiati. I valori di questa colonna sono classificati in ordine discendente.
Top active users	Questo rapporto mostra gli utenti più attivi, classificati in base al numero di file copiati e alla dimensione totale di tutti i file copiati. Per impostazione predefinita, il rapporto include i primi 10 utenti, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene*

TIPO DI RAPPORTO	DESCRIZIONE
	determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server. • **Computer(s):** mostra i computer specificati per il rapporto. • **Channel(s):** mostra i tipi di periferica e/o i protocolli specificati per il rapporto. • **File Name:** mostra i file specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene i principali N (in cui N è un numero specifico) utenti per numero di file copiati. La tabella n° 1 presenta la seguenti colonne: • **User Name** mostra il nome dell'utente. • **Number of Files** mostra il numero di file copiati. I valori di questa colonna sono classificati in ordine discendente. La tabella n° 2 contiene i principali N (in cui N è un numero specifico) utenti per quantità di dati copiati. La tabella n° 2 presenta la seguenti colonne: • **User Name** mostra il nome dell'utente. • **Data Size** mostra la dimensione totale di tutti i file copiati. I valori di questa colonna sono classificati in ordine discendente.
Top copied files	Questo rapporto mostra i file copiati con più frequenza, classificati in base al numero di file copiati e alla dimensione totale di tutti i file copiati. Per impostazione predefinita, il rapporto include i primi 10 file, ma è possibile specificare un numero qualsiasi. Il rapporto è composto da tre sezioni: Intestazione rapporto, Parametri rapporto e Risultati rapporto. La sezione Intestazione rapporto contiene il titolo che compare all'inizio del rapporto. Il titolo indica il tipo di rapporto. La sezione Parametri rapporto contiene informazioni sui parametri del rapporto specificati durante la generazione dello stesso. Queste informazioni includono: • **Period from: to:** mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. *Il formato della data e dell'ora per i campi Period from: e to: viene determinata dal formato dell'account utente su cui viene eseguito DeviceLock Enterprise Server.* • **Computer(s):** mostra i computer specificati per il rapporto. • **Channel(s):** mostra i tipi di periferica e/o i protocolli specificati per il rapporto. • **Users(s):** mostra gli utenti specificati per il rapporto. La sezione Risultati rapporto include due tabelle con i risultati dettagliati del rapporto. La tabella n° 1 contiene i principali N (in cui N è un numero specifico) file copiati per quantità. La tabella n° 1 presenta la seguenti colonne: • **File Name** mostra il nome del file. • **Number of Files** mostra il numero di file copiati. I valori di questa colonna sono classificati in ordine discendente. La tabella n° 2 contiene i principali N (in cui N è un numero specifico) file copiati per dimensione. La tabella n° 2 presenta la seguenti colonne: • **File Name** mostra il nome del file. • **Data Size** mostra la dimensione totale di tutti i file copiati. I valori di

TIPO DI RAPPORTO	DESCRIZIONE
	questa colonna sono classificati in ordine discendente.

Configurazione dell'invio dei rapporti tramite e-mail

DeviceLock consente di distribuire i rapporti tramite e-mail. L'invio dei rapporti tramite e-mail richiede un server SMTP (Simple Mail Transport Protocol). Prima di eseguire l'operazione, occorre specificare il server SMTP da utilizzare per inviare i messaggi e-mail e l'indirizzo e-mail da utilizzare come mittente.

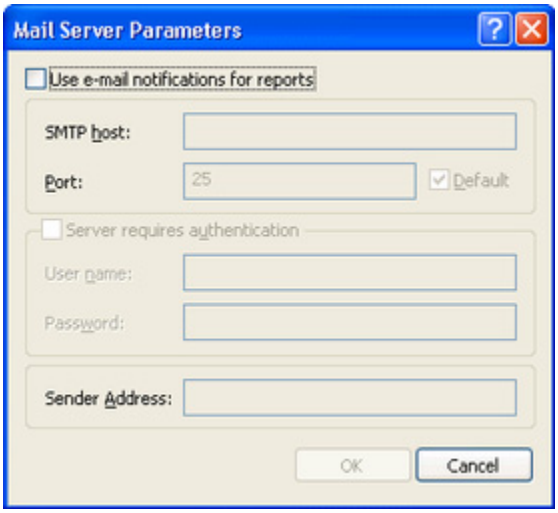
Per configurare l'invio dei rapporti tramite e-mail

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, fare clic con il pulsante destro del mouse su **Reports**, quindi selezionare **Notification Settings**.

   – OPPURE -

   Selezionare **Reports** e fare clic su **Notification Settings** nella barra degli strumenti.

   Viene visualizzata la finestra di dialogo Mail Server Parameter.



4. Nella finestra di dialogo **Mail Server Parameter**, attenersi alle seguenti istruzioni:

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
Use e-mail notifications for reports	Configurare un messaggio di notifica tramite e-mail per i rapporti completati. Selezionare la casella di controllo **Use e-mail notifications for**

UTILIZZARE QUESTA OPZIONE	PER ESEGUIRE QUESTA AZIONE
	reports per digitare le informazioni sulla posta elettronica nelle caselle corrispondenti. Deselezionare la casella di controllo **Use e-mail notifications for reports** per rimuovere le impostazioni sul server SMTP e la notifica e-mail precedentemente configurate.
SMTP host	Specificare il nome del server SMTP da utilizzare per l'invio dei messaggi. È possibile specificare il server SMTP tramite un indirizzo IP o un nome risolvibile DNS.
Port	Specificare la porta utilizzata dai client SMTP per collegarsi al server SMTP. Il valore predefinito è 25.
Server requires authentication	Specificare il tipo di autenticazione da utilizzare con il server SMTP. Selezionare la casella di controllo **Server requires authentication** per specificare l'autenticazione di base. Deselezionare la casella di controllo **Server requires authentication** per non specificare alcuna autenticazione.
User name	Specificare il nome utente da utilizzare per l'autenticazione con il server SMTP. Se è stata specificata l'autenticazione di base, questa proprietà richiede un valore.
Password	Specificare la password da utilizzare per l'autenticazione con il server SMTP. Se è stata specificata l'autenticazione di base, questa proprietà richiede un valore.
Sender Address	Specificare l'indirizzo e-mail da utilizzare nella linea **From:** di un messaggio di posta elettronica.

5. Fare clic su **OK**.

Impostazione del formato predefinito per i rapporti

È possibile specificare il formato di output da utilizzare per i rapporti. Le opzioni disponibili sono:

- Formato HTML (*.htm)
- PDF Format (*.pdf)
- Rich Text Format (*.rtf)

DeviceLock utilizza PDF come formato di output predefinito per i rapporti.

Per impostare il formato predefinito per i rapporti

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, fare clic con il pulsante destro del mouse su **Reports**. Selezionare **Set Default Format**, quindi fare clic su una qualsiasi delle seguenti opzioni: **HTML**, **PDF** o **RTF**.

Definizione dei parametri del rapporto

I parametri del rapporto consentono di specificare i dati provenienti dai file di registro di DeviceLock da utilizzare nel rapporto. Ad esempio, è possibile specificare un intervallo di date per restringere i dati visualizzati nel rapporto. I parametri devono essere impostati per ciascun rapporto singolarmente.

Per definire i parametri del rapporto, utilizzare la finestra di dialogo **Report Options**, che viene visualizzata:

- Facendo clic con il pulsante destro del mouse su un qualsiasi modello di rapporto nella struttura della console e, in seguito, selezionando **New Report**.
- Selezionando uno qualsiasi dei modelli di rapporto nella struttura della console e, in seguito, facendo clic su **New report** nella barra degli strumenti.

Finestra di dialogo Report Options

Period from:……**To:**
mostra la data e l'ora iniziali e finali del periodo del rapporto per cui vengono visualizzati i dati. Il formato della data è *MM/DD/YYYY*, in cui *MM* specifica il mese, *DD* il giorno e *YYYY* l'anno. Il formato dell'ora è *hh:mm:ss {AP}M*, in cui *hh* specifica l'ora, *mm* i minuti, *ss* i secondi e *{AP}M* AM o PM.

Nelle caselle **Period from:** e **To:**, digitare o selezionare la data e l'ora del periodo del rapporto.

L'ora iniziale e finale predefinita del periodo del rapporto è l'ora in cui si apre la finestra di dialogo **Report Options**. La data finale predefinita del periodo del rapporto è la data corrente. La data iniziale predefinita del periodo del rapporto è lo stesso giorno del mese precedente. Ad esempio, se la data corrente è 5 marzo 2009, la data finale predefinita del periodo del rapporto è 3/5/2009, mentre la data iniziale predefinita è 2/5/2009.

Computer(s):
Specifica i computer per il rapporto. La casella **Computer(s)** non viene visualizzata nella finestra di dialogo **Report Options** per i tipi di rapporto Top active computers.

La casella **Computer(s)** è vuota per impostazione predefinita. Ciò significa che il rapporto mostra i dati per tutti i computer nel database di DeviceLock Enterprise Server.

Per specificare i computer per il rapporto, eseguire una qualsiasi delle seguenti azioni:

- Nella casella **Computer(s)**, digitare i nomi di computer utilizzando caratteri jolly come gli asterischi (*) e i punti interrogativi (?). Ad esempio, specificando ***.miodominio.com**, il rapporto mostra i dati relativi a tutti i computer in miodominio.com.

  Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità.

  I nomi di computer multipli vanno separati da una virgola (,) o da un punto e virgola (;).

  - OPPURE -

- Fare clic su **Browse** accanto alla casella **Computer(s):** e attenersi alle seguenti istruzioni:

  a) Quando la finestra di dialogo **Edit computers** list apre l'elenco **Select computer(s)**, selezionare una delle seguenti opzioni:

OPZIONE	DESCRIZIONE
From Database	Questa opzione è selezionata per impostazione predefinita. Questa opzione consente di selezionare i computer dal database di DeviceLock Enterprise Server. Il database contiene tutti i computer da cui il server ha ricevuto dati di controllo e copia shadow. Se viene selezionata questa opzione: 1. Nel riquadro sinistro della finestra di dialogo, selezionare le caselle di controllo relative ai computer desiderati. 2. Fare clic sul pulsante della freccia singola a destra [>]. *I computer selezionati vengono visualizzati nel riquadro destro della finestra di dialogo Selected computers.* *Per rimuovere singoli computer dall'elenco dei computer selezionati, utilizzare il pulsante della freccia singola a sinistra* [<]. *Per aggiungere o rimuovere simultaneamente tutti i computer disponibili verso o dall'elenco dei computer selezionati, utilizzare il pulsante della doppia freccia a destra* [>>] *o della doppia freccia a sinistra* [<<].
From File	Questa opzione consente di selezionare i computer da un file di testo esterno. Il file di testo deve contenere il nome o l'indirizzo IP di ciascun computer in una linea separata e può essere di tipo Unicode o non-Unicode. Se viene selezionata questa opzione: 1. Fare clic sul pulsante dei punti di sospensione [...] per aprire la finestra di dialogo **Open** e cercare il file da usare. 2. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare. 3. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.

OPZIONE	DESCRIZIONE
	4. Fare clic sul file, quindi selezionare **Open**. *I computer inclusi nel file vengono visualizzati nel riquadro sinistro della finestra di dialogo Edit computers*. 5. Nel riquadro sinistro della finestra di dialogo **Edit computers**, selezionare i computer desiderati e fare clic sul pulsante della freccia singola a destra [>]. *I computer selezionati vengono visualizzati nel riquadro destro della finestra di dialogo Selected computers*. *Per rimuovere singoli computer dall'elenco dei computer selezionati, utilizzare il pulsante della freccia singola a sinistra* [<]. *Per aggiungere o rimuovere simultaneamente tutti i computer disponibili verso o dall'elenco dei computer selezionati, utilizzare il pulsante della doppia freccia a destra* [>>] *o della doppia freccia a sinistra* [<<].
Manual	Questa opzione consente di aggiungere manualmente i computer che si desidera selezionare per il rapporto. Se viene selezionata questa opzione: 1. Nel riquadro sinistro della finestra di dialogo **Edit computers list**, digitare i nomi o gli indirizzi IP dei computer. Per posizionare i vari nomi di computer in una linea separata, premere il tasto INVIO dopo aver digitato ciascun nome. 2. Nel riquadro sinistro della finestra di dialogo **Edit computers**, selezionare i computer desiderati e fare clic sul pulsante della freccia singola a destra [>]. *I computer selezionati vengono visualizzati nel riquadro destro della finestra di dialogo Selected computers*. *Per rimuovere singoli computer dall'elenco dei computer selezionati, utilizzare il pulsante della freccia singola a sinistra* [<]. *Per aggiungere o rimuovere simultaneamente tutti i computer disponibili verso o dall'elenco dei computer selezionati, utilizzare il pulsante della doppia freccia a destra* [>>] *o della doppia freccia a sinistra* [<<].

b) Fare clic su **OK**.

Users

Specifica gli utenti per il rapporto. La casella **User(s)** non viene visualizzata nella finestra di dialogo **Report Options** per i tipi di rapporto Top active computers e Top active users.

La casella **User(s)** è vuota per impostazione predefinita. Ciò significa che il rapporto mostra i dati per tutti gli utenti nel database di DeviceLock Enterprise Server.

Per specificare gli utenti per il rapporto, eseguire una qualsiasi delle azioni seguenti:

- Nella casella **User(s)**, digitare nomi di utente utilizzando caratteri jolly come gli asterischi (*) e i punti interrogativi (?). Ad esempio, specificando **miodominio***, il rapporto mostra i dati relativi a tutti gli utenti in miodominio.com.

Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità.

I nomi utente multipli vanno separati da una virgola (,) o da un punto e virgola (;).

Nota: non è possibile specificare gruppi di utenti per il rapporto.

- OPPURE -

- Fare clic su **Browse** accanto alla casella **User(s):** e attenersi alle istruzioni seguenti:
  a) Nella finestra di dialogo **Select Users** visualizzata, nella casella **Enter the object names to select**, digitare il nomi di account utente da specificare per il rapporto.
  I nomi utente multipli vanno separati da un punto e virgola (;).
  b) Fare clic su **OK**.

Threshold
Specifica l'intervallo di tempo, espresso in secondi, tra gli eventi registrati. Questo intervallo viene utilizzato per il consolidamento degli eventi. Compare in tutti i tipi di rapporto della categoria Audit Log, fatta eccezione per Top inserted USB & FireWire devices.

Poiché l'azione di un singolo utente spesso attiva più eventi, DeviceLock utilizza il consolidamento degli eventi mentre li preleva dal registro di controllo allo scopo di redigere rapporti. DeviceLock confronta l'elemento tempo di un evento con quello degli eventi successivi. Se questo intervallo di tempo è inferiore o uguale al valore di **Threshold**, più eventi dello stesso tipo (approvati e negati) vengono combinati in un singolo evento riepilogativo se si verificano tutte le seguenti condizioni:

- Gli eventi sono associati allo stesso computer
- Gli eventi sono associati allo stesso tipo di periferica

Report Devices
Selezionare questa opzione per visualizzare i dati per tutti i tipi di periferica. Se l'opzione non viene selezionata, le informazioni su tutte le attività relative alle periferiche verranno escluse dal rapporto. Compare solo per i tipi di rapporto “Allowed & Denied access requests per channel”, “Allowed vs. Denied access requests” e “Copied files per channel”.

Report Protocols
Selezionare questa opzione per visualizzare i dati per tutti i protocolli. Se l'opzione non viene selezionata, le informazioni su tutte le attività relative ai protocolli verranno escluse dal rapporto. Compare solo per i tipi di rapporto “Allowed & Denied access requests per channel”, “Allowed vs. Denied access requests” e “Copied files per channel”.

Send report via email
Selezionare questa opzione per inviare automaticamente il rapporto generato a singoli utenti tramite e-mail. Se viene selezionata questa opzione, nella casella **Recipients**, digitare gli indirizzi e-mail dei destinatari, separati da virgola, punto e virgola o spazio. Utilizzare il seguente formato: *utente*@*serverdiposta.*

Access type(s)
Specifica i tipi di evento da includere o escludere dal rapporto. Compare solo per il tipo di rapporto Read & Write access requests per device type nella categoria Audit Log.

Selezionando la casella di controllo **Allowed**, gli eventi Success Audit (eventi che registrano tentativi di accesso riusciti) vengono recuperati per il rapporto. Selezionando la casella di controllo **Denied**, gli eventi Failure Audit (eventi che registrano tentativi di accesso non riusciti) vengono recuperati per il rapporto. È possibile utilizzare una di queste due opzioni, o entrambe, per specificare i tipi di evento.

Device type(s)
Specifica i tipi di periferica per il rapporto. Compare solo per i tipi di rapporto Top active computers, Top active users e Top copied files.

In caso di utilizzo di questa opzione, selezionare le caselle di controllo appropriate accanto ai tipi di periferica da specificare per il rapporto.

Protocol(s)
Specifica i protocolli per il rapporto. Compare solo per i tipi di rapporto "Top active computers", "Top active users" e "Top copied files".

In caso di utilizzo di questa opzione, selezionare le caselle di controllo pertinenti accanto ai protocolli da specificare per il rapporto.

Nota: se non viene selezionata alcuna delle opzioni **Device type(s)** e **Protocol(s)**, il rapporto mostra i dati relativi a tutti i tipi di periferica e a tutti i protocolli. Se viene selezionata una delle opzioni e, in seguito, vengono specificati i tipi di periferica o i protocolli, il rapporto mostra unicamente i dati relativi ai tipi di periferica o ai protocolli specificati.

Top computers
Specifica la quantità dei computer utilizzati con più frequenza. Compare solo per il tipo di rapporto Top active computers.

Il valore predefinito è 10. Per modificare il valore predefinito, digitare o selezionare il numero desiderato di computer nella casella **Top computers**.

Top users
Specifica la quantità degli utenti più attivi. Compare solo per il tipo di rapporto Top active users.

Il valore predefinito è 10. Per modificare il valore predefinito, digitare o selezionare il numero desiderato di utenti nella casella **Top users**.

Top USB and FireWire devices
Specifica la quantità delle periferiche USB e FireWire inserite con più frequenza Compare solo per il tipo di rapporto Top inserted USB & FireWire devices.

Il valore predefinito è 10. Per modificare il valore predefinito, digitare o selezionare il numero desiderato di periferiche nella casella **Top USB and FireWire devices**.

Top USB devices
Specifica la quantità delle periferiche USB utilizzate con più frequenza Compare solo per il tipo di rapporto Top used USB devices.

Il valore predefinito è 10. Per modificare il valore predefinito, digitare o selezionare il numero desiderato di periferiche nella casella **Top USB devices**.

File name
Specifica i file per il rapporto. Compare solo per i tipi di rapporto Top active users, Top active computers e Copied files per channel nella categoria Shadow Log.

La casella **File name** è vuota per impostazione predefinita. Ciò significa che il rapporto mostra i dati per tutti i file nel database di DeviceLock Enterprise Server.

Per specificare i file per il rapporto, nella casella **File name**, digitare i nomi di file utilizzando caratteri jolly come gli asterischi (*) e i punti interrogativi (?). Ad esempio, digitare ***.txt** per specificare tutti i file con estensione .txt. Se, invece, si desidera specificare tutti i file il cui nome inizia con qualsiasi carattere contenente la stringa "prezzo", indipendentemente dall'estensione, digitare ***prezzo*.***

Un asterisco (*) sostituisce un numero illimitato di caratteri. Il punto interrogativo (?) sostituisce un singolo carattere. È possibile utilizzare i caratteri jolly in qualsiasi posizione e quantità.

I nomi di file multipli vanno separati da una virgola (,) o da un punto e virgola (;).

Gestione dei rapporti

La gestione dei rapporti di DeviceLock include le seguenti attività:

- Esecuzione dei rapporti
- Aggiornamento dei rapporti
- Visualizzazione dei rapporti
- Visualizzazione dei parametri dei rapporti
- Esportazione e salvataggio dei rapporti
- Invio dei rapporti tramite e-mail
- Eliminazione dei rapporti

Esecuzione dei rapporti

Per eseguire un rapporto

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, fare clic con il pulsante destro del mouse su qualsiasi modello di rapporto da utilizzare, quindi selezionare **New report**.

   Viene visualizzata la finestra di dialogo Report Options.
6. Nella finestra di dialogo **Report Options**, accettare o modificare le impostazioni predefinite, quindi fare clic su **OK**.

   Per informazioni sulle impostazioni predefinite e su come modificarle nella finestra di dialogo Report Options, consultare la sezione "Definizione dei parametri del rapporto".

   Mentre il rapporto viene elaborato su DeviceLock Enterprise Server, le informazioni sull'esecuzione dello stesso vengono visualizzate su DeviceLock Management Console. Per consultare e analizzare queste informazioni, nella struttura della console selezionare il modello di rapporto utilizzato per eseguire un nuovo rapporto.

   Nel riquadro dei dettagli vengono visualizzate le informazioni di esecuzione riguardanti tutti i rapporti basati sul modello selezionato. Le informazioni di esecuzione del rapporto includono:

   - **User** Nome dell'utente che ha eseguito il rapporto.
   - **From Computer** Nome del computer utilizzato per eseguire il rapporto.
   - **Started** Data e ora d'inizio dell'esecuzione del rapporto.
   - **Finished** Data e ora del completamento del rapporto.
   - **E-mailed** Valori possibili: **Yes** e **No**. **Yes** indica che il rapporto selezionato per la consegna tramite e-mail è stato consegnato correttamente ad alcuni o a tutti i destinatari desiderati. **Yes** viene visualizzato solo dopo il completamento del processo di invio. **No** indica che:

     Il rapporto non è stato incluso nella consegna tramite e-mail.

     - OPPURE -

     Il rapporto è stato incluso nella la consegna tramite e-mail ma non ha raggiunto tutti i destinatari specificati.

In presenza di un errore durante la consegna di un rapporto tramite e-mail, è possibile ricorrere a Server Log Viewer per determinarne il motivo. Per maggiori informazioni, consultare la sezione "Server Log Viewer".

Se sul computer in uso è in esecuzione un software anti-virus o anti-spamming e si verifica un errore durante la consegna di un rapporto tramite e-mail, le informazioni sull'errore non possono essere incluse nel registro di DeviceLock Enterprise Server. Ciò accade in quanto i prodotti anti-virus e anti-spamming (ad esempio Symantec Norton AntiVirus) possono intercettare automaticamente il traffico e-mail.

Per informazioni sul funzionamento del proprio programma anti-virus/anti-spamming utilizzato, consultare la documentazione inclusa con il programma.

- **Status** Valori possibili: **Generating**, **Ready**, **Error**. **Generating** indica che il rapporto è in fase di generazione. **Ready** indica che il rapporto è stato completato correttamente. **Error** indica che si è verificato un errore durante la generazione del rapporto.
  In tal caso, attenersi alle seguenti istruzioni per determinarne il motivo:
  Fare clic sul rapporto per visualizzare il messaggio di errore.
  - OPPURE -
  Utilizzare Server Log Viewer. Per maggiori informazioni, consultare la sezione "Server Log Viewer"

Aggiornamento dei rapporti

Poiché i rapporti correnti e il loro stato non vengono aggiornati automaticamente, è necessario eseguire un'operazione di aggiornamento.

Per aggiornare i rapporti

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, fare clic con il pulsante destro del mouse su qualsiasi modello di rapporto, quindi selezionare **Refresh**.

   - OPPURE -

   Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare i rapporti ed eseguire una delle seguenti azioni:

   - Fare clic su **Refresh** sulla barra degli strumenti.
     - OPPURE -
   - Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi rapporto, quindi selezionare **Refresh**.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

Visualizzazione dei rapporti

Una volta completato correttamente, è possibile aprire un rapporto in DeviceLock Management Console.

Per visualizzare un rapporto

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare il rapporto che si desidera visualizzare.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

6. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul rapporto che si desidera visualizzare e selezionare **Open**.

   Il rapporto viene aperto nell'applicazione associata con il formato del rapporto predefinito selezionato. Per impostazione predefinita, il rapporto viene aperto con Adobe Acrobat Reader, in quanto DeviceLock utilizza PDF come formato di output predefinito per i rapporti.

   Per aprire un rapporto in formato PDF, sul computer in uso deve essere installato Adobe Acrobat Reader. È possibile scaricare il programma sul sito Web di Adobe: http://get.adobe.com/reader/.

Visualizzazione dei parametri dei rapporti

Dopo aver eseguito un rapporto, è possibile ottenere informazioni sui parametri specificati durante la generazione del rapporto.

Per visualizzare i parametri del rapporto

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare il rapporto.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

6. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul rapporto, quindi selezionare **View parameters**.

Viene visualizzata la finestra di dialogo Report Options. In questa finestra di dialogo è possibile visualizzare i valori dei parametri specificati durante la generazione del rapporto.

Esportazione e salvataggio dei rapporti

DeviceLock consente di esportare i rapporti generati in altri formati (come HTML, PDF o RTF) e di salvarli localmente o in rete.

Nota: durante il salvataggio di tipo HTML, il report viene salvato in formato .htm. Se il report contiene immagini grafiche, ciascuna immagine viene salvata in formato .gif nella stessa directory del file .htm.

Per esportare e salvare i rapporti

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare il rapporto che si desidera esportare e salvare.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

6. Per esportare e salvare un solo rapporto:

   a) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul rapporto che si desidera esportare e salvare, selezionare **Save As**, quindi fare clic su una qualsiasi delle seguenti opzioni: **HTML**, **PDF** o **RTF**.
   Viene visualizzata la finestra di dialogo Save As.

   b) Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il rapporto.

   c) Nella casella **File name**, digitare il nome di file desiderato.
   Per impostazione predefinita, il nome del file è {Tipo_rapporto}- [{gg.mm.aa oo:mm:ss}], in cui {gg.mm.aa oo:mm:ss} rappresenta la data e l'ora correnti.

   d) Fare clic su **Save**.

   Se il report salvato in formato HTML contiene una o più immagini grafiche, le immagini vengono estratte dal report e salvate separatamente in formato .gif nella stessa directory del file .htm.

   Per esportare e salvare più di un rapporto:

   a) Nel riquadro dei dettagli, selezionare più rapporti tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui rapporti.

   b) Fare clic con il pulsante destro del mouse sulla selezione, fare clic su **Save As**, quindi scegliere una qualsiasi delle seguenti opzioni: **HTML**, **PDF** o **RTF**.
   Viene visualizzata la finestra di dialogo Browse for folder.

c) Nella finestra di dialogo **Browse for folder**, selezionare la cartella in cui salvare i rapporti, quindi fare clic su **OK**.

Invio dei rapporti tramite e-mail

DeviceLock consente di inviare i rapporti generati tramite e-mail.

Per inviare i rapporti generati tramite e-mail

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.
5. Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare il rapporto che si desidera inviare tramite e-mail.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

6. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul rapporto che si desidera inviare e selezionare **Send via e-mail**.

   È possibile selezionare più rapporti tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui rapporti.

   Viene visualizzata la finestra di dialogo Send report via e-mail.

7. Nella finestra di dialogo **Send report via e-mail**, nella casella **Recipients**, digitare gli indirizzi e-mail dei destinatari, separati da virgola, punto e virgola o spazio. Utilizzare il seguente formato: *utente*@*serverdiposta.*
8. Fare clic su **OK**.

   In presenza di un errore durante la consegna di un rapporto tramite e-mail, viene registrato un messaggio di errore pertinente. Per determinarne il motivo, è possibile ricorrere a Server Log Viewer. Per maggiori informazioni, consultare la sezione "Server Log Viewer".

Nota: quando viene inviato un report in formato HTML, il report viene inserito nel corpo del messaggio di posta elettronica e non come allegato.

Eliminazione dei rapporti

Quando i rapporti non sono più necessari, possono essere eliminati.

Per eliminare i rapporti

1. Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Enterprise Server.
2. Nella struttura della console, espandere **DeviceLock Enterprise Server**.
3. Sotto **DeviceLock Enterprise Server**, espandere **Reports**.
4. Espandere **Audit Log** o **Shadow Log**.

5. Sotto **Audit Log** o **Shadow Log**, selezionare il modello utilizzato per generare il rapporto che si desidera eliminare.

   Selezionando un modello di rapporto nella struttura della console, è possibile visualizzare i rapporti associati con lo stesso nel riquadro dei dettagli.

6. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul rapporto che si desidera eliminare e selezionare **Delete**.

   È possibile eliminare più rapporti simultaneamente nel seguente modo:

   a) Nel riquadro dei dettagli, selezionare più rapporti tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui rapporti.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Delete**.

Criteri di protezione di DeviceLock (Offline Profile)

Nelle organizzazioni moderne, molti utenti necessitano dell'accesso ai dati di primaria importanza anche quando non sono collegati alla rete aziendale. Ad esempio, i rappresentanti delle vendite, gli agenti assicurativi e gli ispettori regionali usano sempre più laptop o notebook aziendali quando sono fuori sede. La protezione dei dati riservati su questi dispositivi mobili è diventata una priorità per molte organizzazioni.

DeviceLock assicura una protezione avanzata dei dati riservati aziendali negli ambienti fuori rete. Ora è possibile controllare l'accesso degli utenti alle periferiche, ai protocolli e alle copie shadow dei dati scritti dall'utente o trasmessi sulla rete in diversi scenari offline. DeviceLock, inoltre, offre una maggiore flessibilità di gestione, consentendo di definire diversi criteri di sicurezza online od offline per lo stesso utente o gli stessi gruppi di utenti.

I criteri online vengono applicati quando l'utente è collegato alla rete aziendale o a specifici DeviceLock Enterprise Server e controller di dominio Active Directory. I criteri offline utente vengono applicati quando l'utente lavora fuori sede e non è collegato alla rete aziendale o a specifici DeviceLock Enterprise Server e controller di dominio Active Directory.

Per configurare DeviceLock affinché applichi diversi criteri a seconda degli scenari online e offline, occorre innanzitutto impostare le autorizzazioni per i due tipi di profilo:

- **Regular Profile** (Profilo normale). Queste impostazioni vengono utilizzate dai computer client che operano online.
- **Offline Profile** (Profilo offline). Queste impostazioni vengono utilizzate dai computer client che operano offline, ad esempio i laptop usati dai dipendenti che lavorano fuori sede. Se le impostazioni di Offline Profile non sono configurate, vengono usate quelle di Regular Profile.

Si possono utilizzare diversi profili regolari od offline per le seguenti funzioni: Permissions (Autorizzazioni), Auditing and Shadowing (Controllo e Shadowing), USB Devices White List (Lista bianca delle periferiche USB), Media White List (Lista bianca unità), Protocols White List (Lista bianca dei protocolli), Content-Aware Rules (Regole basate sul contenuto) e Security Settings (Impostazioni di protezione). È possibile gestire le impostazioni del profilo offline utilizzando DeviceLock Management Console, DeviceLock Service Settings Editor o DeviceLock Group Policy Manager.

I seguenti esempi descrivono gli scenari tipici in cui impostare i criteri di protezione online od offline per garantire la sicurezza dei dati aziendali.

- **Scenario 1.** Si supponga di disporre di un team finanziario nella propria organizzazione. L'amministratore autorizza i membri del team a scrivere file sui dispositivi Removable, DVD/CD-ROM, USB e Floppy mentre lavorano online. La loro attività online viene controllata. Per tutti i file copiati viene eseguita la copia shadow e i registri di controllo e shadowing vengono inviati a DeviceLock Enterprise Server.

Per i membri del team finanziario che lavorano offline l'accesso in scrittura non è autorizzato.

Questi criteri di protezione consentono di monitorare le attività dei membri del team finanziario in tempo reale. Esaminando i registri di controllo e di copia shadow su DeviceLock Enterprise Server (spesso con frequenza giornaliera), è possibile reagire in maniera rapida ed appropriata in caso di perdite di dati. In uno scenario del genere, un utente non può copiare dati riservati su una periferica mentre lavora offline. Il tentativo di evitare di inviare le copie shadow a DeviceLock Enterprise Server metterebbe in allarme il reparto responsabile della sicurezza.

- **Scenario 2.** Laura lavora come rappresentante delle vendite in una grande azienda e durante i suoi frequenti viaggi fuori sede usa un notebook aziendale. Per svolgere correttamente il suo lavoro, Laura deve poter trasmettere ai suoi partner commerciali i file di dati riguardanti le sue attività. In una situazione del genere, è possibile concedere a Laura l'accesso in scrittura ad alcuni file nelle periferiche Removable, DVD/CD-ROM, USB e Floppy, autorizzando la copia shadow di questi file mentre lavora offline. Mentre lavora online, invece, Laura non dispone dell'accesso in scrittura per i tipi di periferica specificati.

  Questi criteri di protezione assicurano una grande flessibilità nella gestione degli accessi degli utenti, garantendo allo stesso tempo la sicurezza dei dati aziendali.

Configurazione delle impostazioni di rilevamento in modalità offline

È possibile definire le caratteristiche di rete utilizzate da DeviceLock per rilevare lo stato di connessione (online od offline). Per impostazione predefinita, DeviceLock opera in modalità offline se un cavo di rete non è collegato al computer client.

Come configurare le impostazioni di rilevamento in modalità offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

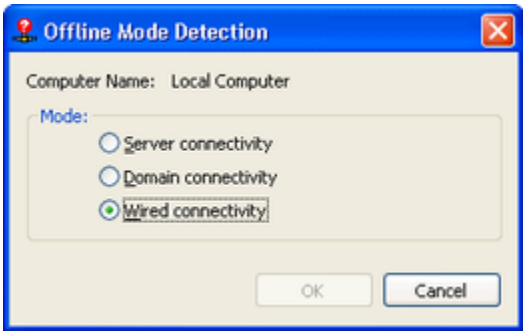
   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Selezionare **Service Options**.

   Dopo aver selezionato Service Options nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

3. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse su **Offline mode detection**, quindi scegliere **Properties**.
  - OPPURE -
- Fare doppio clic su **Offline mode detection**.

Viene visualizzata la finestra di dialogo Offline Mode Detection.



4. Nella finestra di dialogo **Offline Mode Detection**, selezionare una qualsiasi delle seguenti opzioni:

OPZIONE	DESCRIZIONE
Server connectivity	Indica che lo stato di connessione di un computer client dipende dalla possibilità di collegarsi o meno a un determinato DeviceLock Enterprise Server. Di conseguenza, un computer client opera in modalità online se può collegarsi a uno qualsiasi dei DeviceLock Enterprise Server specificati e inviare registri di controllo e shadowing ai server. Un computer client opera in modalità offline se non può collegarsi tramite autenticazione a nessuno dei DeviceLock Enterprise Server specificati o se tutti i DeviceLock Enterprise Server specificati risultano non disponibili contemporaneamente. **Procedura consigliata:** il modo più affidabile per proteggere la comunicazione client/server è l'utilizzo dell'autenticazione tramite certificato di DeviceLock. Per l'autenticazione tramite certificato client/server, la chiave pubblica deve essere installata sui computer client, mentre la chiave privata sui DeviceLock Enterprise Server. Se il certificato (la chiave pubblica) viene installato solo su DeviceLock Enterprise Server, il server respinge le connessioni e i computer client operano in modalità offline. Se il certificato (la chiave pubblica) è installato solo sui computer client, il server e il client si autenticano a vicenda quando viene stabilita una connessione. Tuttavia, questa autenticazione è meno sicura rispetto a quella basata su un certificato. Per informazioni dettagliate sui certificati di DeviceLock, consultare la sezione "Certificati di DeviceLock".

OPZIONE	DESCRIZIONE
Domain connectivity	Indica che lo stato di connessione di un computer client dipende dalla possibilità di collegarsi o meno al controller di dominio Active Directory appropriato (controller del dominio a cui appartiene il computer client). Di conseguenza, un computer client opera in modalità online se può collegarsi al controller di dominio appropriato. Un computer client opera in modalità offline se il controller di dominio appropriato non è disponibile. *Un computer client che non appartiene a un dominio (un computer di un gruppo di lavoro o stand-alone) opera sempre in modalità offline.*
Wired connectivity	Indica che lo stato di connessione di un computer client dipende dal collegamento o meno del cavo di rete alla scheda di interfaccia di rete (NIC). Si tratta del metodo più semplice e meno sicuro per rilevare lo stato di connessione. Di conseguenza, un computer client opera in modalità online se il cavo di rete è collegato alla scheda NIC. Un computer client opera in modalità offline se il cavo di rete non è collegato alla scheda NIC. Si noti che le connessioni di rete wireless (ad esempio Wi-Fi) e ai modem sono ignorate. Questa opzione è selezionata per impostazione predefinita.

5. Fare clic su **OK**.

Passaggio dalla modalità online a quella offline e viceversa

DeviceLock Service in esecuzione sui computer client rileva automaticamente lo stato di connessione e alterna senza interruzioni la modalità online e offline ogni ora e se si verifica uno dei seguenti eventi:

- Un utente avvia il computer in cui è in esecuzione DeviceLock Service.
  DeviceLock Service viene sempre avviato in modalità offline.
- Un utente esegue l'accesso.
- Un utente fa clic con il pulsante destro del mouse sull'icona DeviceLock Tray Notification Utility nell'area di notifica della barra delle applicazioni, quindi seleziona **Refresh Current State**.
  L'icona DeviceLock Tray Notification Utility viene visualizzata nell'area di notifica se l'opzione Always show tray icon viene attivata in Service Options.
- DeviceLock Service invia registri di controllo e di copia shadow a DeviceLock Enterprise Server.
- Un'interfaccia di rete cambia di stato:
  - Un cavo di rete viene collegato o scollegato.
  - Un modem viene collegato e scollegato.
  - Una connessione di rete privata virtuale (VPN) viene stabilita o terminata.

  - Una connessione di rete wireless tramite scheda Wi-Fi viene stabilita o terminata.
  - Un indirizzo IP assegnato dal DHCP viene usato o rilasciato.
  - Una scheda di rete viene abilitata, disabilitata, aggiunta o rimossa.

- Vengono apportate delle modifiche alle impostazioni di DeviceLock Service.

Gestione dei criteri di protezione offline per le periferiche

La gestione dei criteri di protezione offline è molto simile a quella dei criteri online (regolare), tranne per alcune differenze. In questa sezione vengono fornite informazioni sul profilo offline e sulle procedure di gestione di base. Per informazioni dettagliate su autorizzazioni, regole di controllo e shadowing, liste bianche, regole basate sul contenuto e impostazioni di protezione, consultare le seguenti sezioni del manuale utente: "Autorizzazioni (Regular Profile)", "Controllo e shadowing (Regular Profile)", "Lista bianca delle periferiche USB (Regular Profile)", "Lista bianca delle unità (Regular Profile)", "Impostazioni di protezione (Regular Profile)", "Regole basate sul contenuto per le periferiche (Regular Profile)".

La gestione dei criteri di protezione offline per le periferiche prevede le seguenti operazioni:

- Gestione delle autorizzazioni offline
- Gestione delle regole di controllo e shadowing offline
- Gestione della lista bianca delle periferiche USB offline
- Gestione della lista bianca delle unità offline
- Gestione delle regole basate sul contenuto offline
- Gestione delle impostazioni di protezione offline

È possibile gestire i criteri di protezione offline utilizzando DeviceLock Management Console, Service Settings Editor o DeviceLock Group Policy Manager.

Gestione delle autorizzazioni offline

Per una descrizione dettagliata della funzione Permissions (Autorizzazioni), consultare la sezione "Permissions (Regular Profile)".

Le autorizzazioni offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le autorizzazioni per un tipo di periferica non sono state configurate. Si tratta dello stato predefinito.
Configured	Indica che le autorizzazioni per un tipo di periferica sono state configurate.

STATO	DESCRIZIONE
Full Access	Indica che i diritti di accesso completi sono garantiti all'account Everyone.
No Access	Indica una delle seguenti condizioni: • L'account Everyone dispone delle autorizzazioni di tipo No Access (Nessun accesso) ed è l'unico account assegnato a un tipo di periferica. *Le autorizzazioni No Access assegnate all'account Everyone hanno la priorità sulle autorizzazioni assegnate agli altri account.* • Tutti gli utenti e i gruppi assegnati a un tipo di periferica hanno le autorizzazioni di tipo No Access. • Tutti gli utenti e i gruppi assegnati a un tipo di periferica sono stati rimossi.
Use Regular	Indica che l'eredità delle autorizzazioni offline è bloccata e sono applicate le autorizzazioni Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle autorizzazioni normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle autorizzazioni normali consente di evitare che le autorizzazioni offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle autorizzazioni normali, consultare la sezione "Rimozione delle autorizzazioni offline".

La gestione delle autorizzazioni offline include le seguenti attività:

- Impostazione e modifica delle autorizzazioni offline
- Rimozione della definizione delle autorizzazioni offline
- Rimozione delle autorizzazioni offline

Impostazione e modifica delle autorizzazioni offline

Come impostare e modificare le autorizzazioni offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

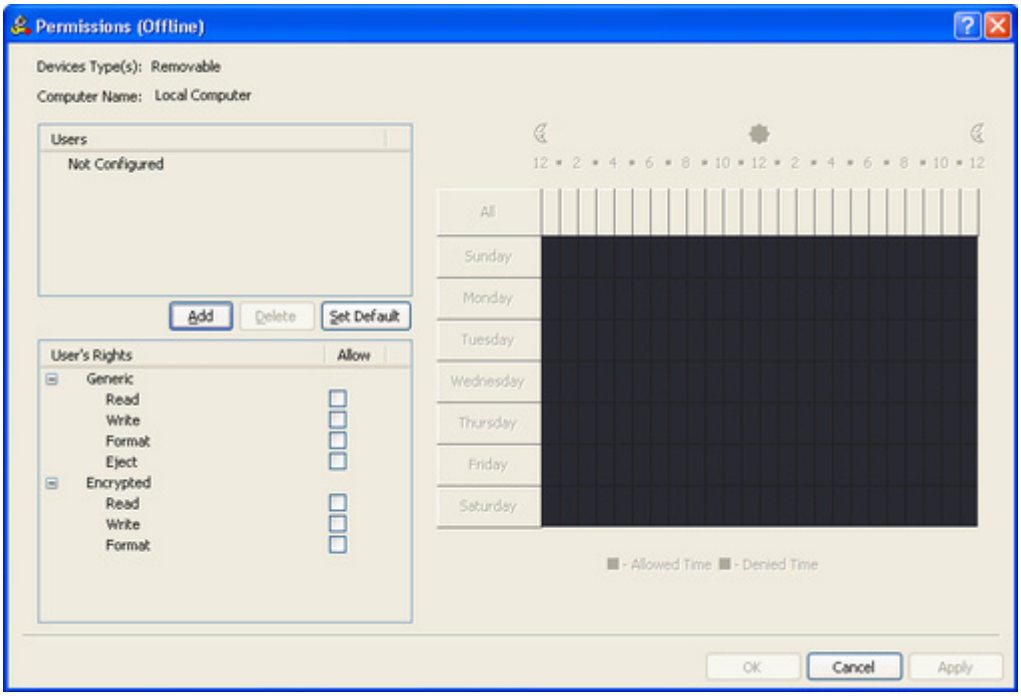
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Permissions**.

   Dopo aver selezionato Permissions (Autorizzazioni) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun tipo di periferica.

4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera impostare o modificare le autorizzazioni, quindi scegliere **Set Offline Permissions**.

     - OPPURE -
   - Selezionare il tipo di periferica per cui si desidera impostare o modificare le autorizzazioni, quindi fare clic su **Set Offline Permissions** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Permissions (Offline).



5. Nella finestra di dialogo **Permissions (Offline)**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Impostare le autorizzazioni predefinite	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**. *Le autorizzazioni predefinite sono assegnate agli account Administrators, Everyone e SYSTEM. Per informazioni sulle autorizzazioni assegnate a questi account per impostazione predefinita, consultare la sezione "Permissions (Regular Profile)".*

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Impostare le autorizzazioni per un ulteriore utente o gruppo	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 2. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Permissions (Offline).* 3. Nel riquadro superiore sinistro della finestra di dialogo **Permissions (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti e/o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.* 4. Nel riquadro inferiore sinistro della finestra di dialogo **Permissions (Offline)**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati. *Nel riquadro destro della finestra di dialogo Permissions (Offline), è possibile impostare le restrizioni per data e ora, al fine di limitare l'accesso alle periferiche da parte dell'utente. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui l'utente o il gruppo selezionato possono accedere alle periferiche. Utilizzare il pulsante destro del mouse per selezionare i giorni e le ore in cui l'utente o il gruppo selezionato non possono accedere alle periferiche*.
Modificare le autorizzazioni per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati.
Rimuovere un utente o gruppo esistente e le autorizzazioni	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle autorizzazioni offline

È possibile riportare le autorizzazioni offline precedentemente definite allo stato non configurato. Se le autorizzazioni non sono definite, ai computer client offline vengono applicate le autorizzazioni normali.

Come rimuovere la definizione delle autorizzazioni offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Permissions**.

   Dopo aver selezionato Permissions (Autorizzazioni) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun tipo di periferica.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera rimuovere la definizione delle autorizzazioni offline, quindi selezionare **Undefine Offline**.

   È possibile rimuovere simultaneamente la definizione delle autorizzazioni offline impostate per più tipi di periferica nel seguente modo:

   a) Nel riquadro dei dettagli, selezionare più tipi di periferica tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui tipi di periferica.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine Offline**.

   Lo stato offline delle autorizzazioni cambia in "Not Configured" (Non configurato).

Rimozione delle autorizzazioni offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle autorizzazioni offline di livello superiore e applicare le autorizzazioni normali a specifici gruppi di computer client di livello inferiore. Per applicare le autorizzazioni normali, occorre rimuovere le autorizzazioni offline.

Come rimuovere le autorizzazioni offline

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.

b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Permissions**.

   Dopo aver selezionato Permissions (Autorizzazioni) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun tipo di periferica.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera rimuovere le autorizzazioni offline, quindi selezionare **Remove Offline**.

   È possibile rimuovere simultaneamente le autorizzazioni offline impostate per più tipi di periferica nel seguente modo:

   a) Nel riquadro dei dettagli, selezionare più tipi di periferica tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui tipi di periferica.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Remove Offline**.

   Lo stato offline delle autorizzazioni cambia in "Use Regular" (Usa normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle regole di controllo e shadowing offline

Per una descrizione dettagliata della funzione Auditing & Shadowing (Controllo e shadowing), consultare la sezione "Auditing & Shadowing (Regular Profile)".

Le regole di controllo e shadowing offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le regole di controllo e shadowing non sono definite per un tipo di periferica. Si tratta dello stato predefinito.
Configured	Indica che le regole di controllo e shadowing sono definite per un tipo di periferica.
No Audit	Indica una delle seguenti condizioni: • I diritti di Audit (Controllo) non sono impostati per tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un tipo di periferica. • Tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un tipo di periferica sono stati rimossi. • L'account Everyone non dispone dei diritti Audit e Shadowing ed è l'unico account specificato nelle regole di controllo e shadowing per un tipo di periferica.

STATO	DESCRIZIONE
Use Regular	Indica che l'eredità delle regole di controllo e shadowing offline è bloccata e sono applicate le regole di controllo e shadowing Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle regole normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle regole normali consente di evitare che le regole offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle regole normali, consultare la sezione "Rimozione delle regole di controllo e shadowing offline".

La gestione delle regole di controllo e shadowing offline include le seguenti attività:

- Definizione e modifica delle regole di controllo e shadowing offline
- Rimozione della definizione delle regole di controllo e shadowing offline
- Rimozione delle regole di controllo e shadowing offline

Definizione e modifica delle regole di controllo e shadowing offline

Come definire e modificare le regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing (Controllo e shadowing) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun tipo di periferica.

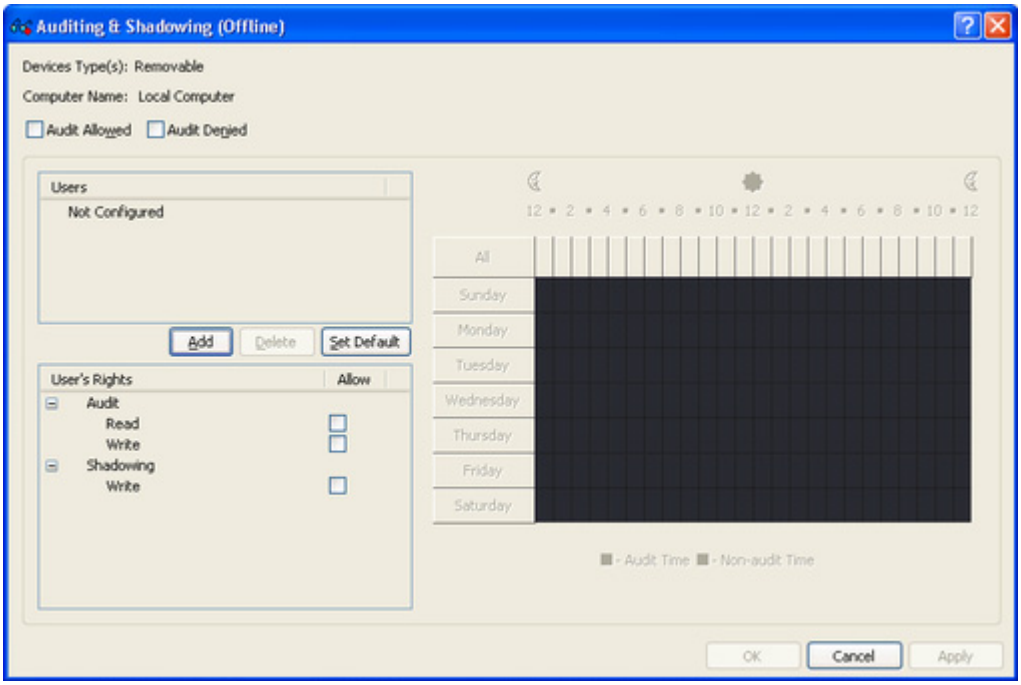
4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera definire o modificare le regole, quindi scegliere **Set Offline Auditing & Shadowing**.

  - OPPURE -

- Selezionare il tipo di periferica per cui si desidera definire o modificare le regole, quindi fare clic su **Set Offline Auditing & Shadowing** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Auditing & Shadowing (Offline).



5. Nella finestra di dialogo **Auditing & Shadowing (Offline)**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Definire le regole di controllo e shadowing offline	1. Nel riquadro superiore sinistro della finestra di dialogo, specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a una periferica andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a una periferica non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**. *Le regole di controllo e shadowing predefinite si applicano ai membri del gruppo Users e all'account Everyone. Per informazioni sulle regole di controllo e shadowing assegnate a questi account per impostazione predefinita, consultare la sezione "Auditing & Shadowing (Regular Profile)".*

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Definire le regole di controllo e shadowing per un ulteriore utente o gruppo	1. Nel riquadro superiore sinistro della finestra di dialogo, specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a una periferica andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a una periferica non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 3. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Auditing & Shadowing (Offline)*. 4. Nel riquadro superiore sinistro della finestra di dialogo **Auditing & Shadowing (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti e/o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi*. 5. Nel riquadro inferiore sinistro della finestra di dialogo **Auditing & Shadowing (Offline)**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di controllo e shadowing appropriati. *I diritti di controllo e shadowing determinano le azioni eseguite dall'utente sulle periferiche che vanno inserite nei registri di controllo e/o shadowing*. *Nel riquadro destro della finestra di dialogo Auditing & Shadowing (Offline), si possono specificare i giorni e le ore (ad esempio, dalle 7 alle 17, dal lunedì al venerdì) in cui le azioni eseguite sulle periferiche dall'utente selezionato vanno inserite nel registro di controllo o shadowing. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui le azioni eseguite sulle periferiche dall'utente selezionato vanno registrate. Utilizzare il pulsante destro del mouse per selezionare i giorni e le ore in cui le azioni eseguite sulle periferiche dall'utente selezionato non vanno registrate*.
Modificare le regole di controllo e shadowing per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di controllo e shadowing appropriati.
Rimuovere un utente o gruppo esistente e la regola	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle regole di controllo e shadowing offline

È possibile riportare le regole di controllo e shadowing offline precedentemente definite allo stato non configurato. Se le regole offline non sono definite, ai computer client offline vengono applicate le regole normali.

Come rimuovere la definizione delle regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing (Controllo e shadowing) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun tipo di periferica.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera rimuovere la definizione delle regole di controllo e shadowing offline, quindi selezionare **Undefine Offline**.

   È possibile rimuovere simultaneamente la definizione delle regole di controllo e shadowing definite per più tipi di periferica nel seguente modo:
   a) Nel riquadro dei dettagli, selezionare più tipi di periferica tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui tipi di periferica.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine Offline**.

   Lo stato offline delle regole di controllo e shadowing cambia in "Not Configured" (Non configurato).

Rimozione delle regole di controllo e shadowing offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle regole di controllo e

shadowing offline di livello superiore e applicare le regole di controllo e shadowing normali a specifici gruppi di computer client di livello inferiore. Per applicare le regole di controllo e shadowing Regular (normali), occorre rimuovere le regole di controllo e shadowing offline.

Come rimuovere le regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing (Controllo e shadowing) nella struttura della console, nel riquadro dei dettagli vengono visualizzati i tipi di periferica per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun tipo di periferica.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul tipo di periferica per cui si desidera rimuovere le regole di controllo e shadowing offline, quindi selezionare **Remove Offline**.

   È possibile rimuovere simultaneamente le regole di controllo e shadowing definite per più tipi di periferica nel seguente modo:
   a) Nel riquadro dei dettagli, selezionare più tipi di periferica tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui tipi di periferica.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Remove Offline**.

   Lo stato offline delle regole di controllo e shadowing cambia in "Use Regular" (Usa normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione della lista bianca delle periferiche USB offline

Per una descrizione dettagliata della funzione USB Devices White List (Lista bianca periferiche USB), consultare la sezione "USB Devices White List (Regular Profile)".

La lista bianca delle periferiche USB offline può presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che la lista bianca non è definita. Viene visualizzato il messaggio "Offline USB White List is not configured" (La lista bianca delle periferiche USB offline non

STATO	DESCRIZIONE
	è configurata). Si tratta dello stato predefinito.
Configured	Indica che la lista bianca è definita.
Use Regular	Indica che l'eredità della lista bianca offline è bloccata ed è applicata la lista bianca Regular (normale). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione della lista bianca normale è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione della lista bianca normale consente di evitare che la lista bianca offline ereditata da un livello superiore venga applicata a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione della lista bianca normale, consultare la sezione "Rimozione della lista bianca delle periferiche USB offline".

La gestione della lista bianca delle periferiche USB offline include le seguenti attività:

- Definizione e modifica della lista bianca delle periferiche USB offline
- Esportazione e importazione della lista bianca delle periferiche USB offline
- Rimozione della definizione della lista bianca delle periferiche USB offline
- Rimozione della lista bianca delle periferiche USB offline

Definizione e modifica della lista bianca delle periferiche USB offline

Come definire e modificare la lista bianca delle periferiche USB offline

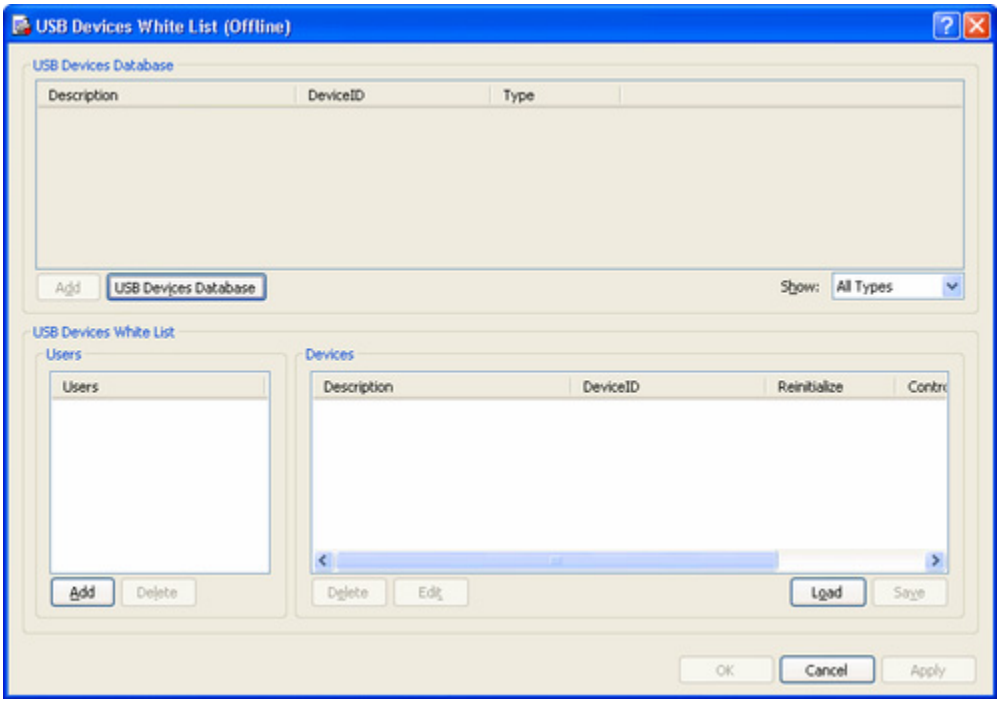
1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Manage Offline**.
     - OPPURE -

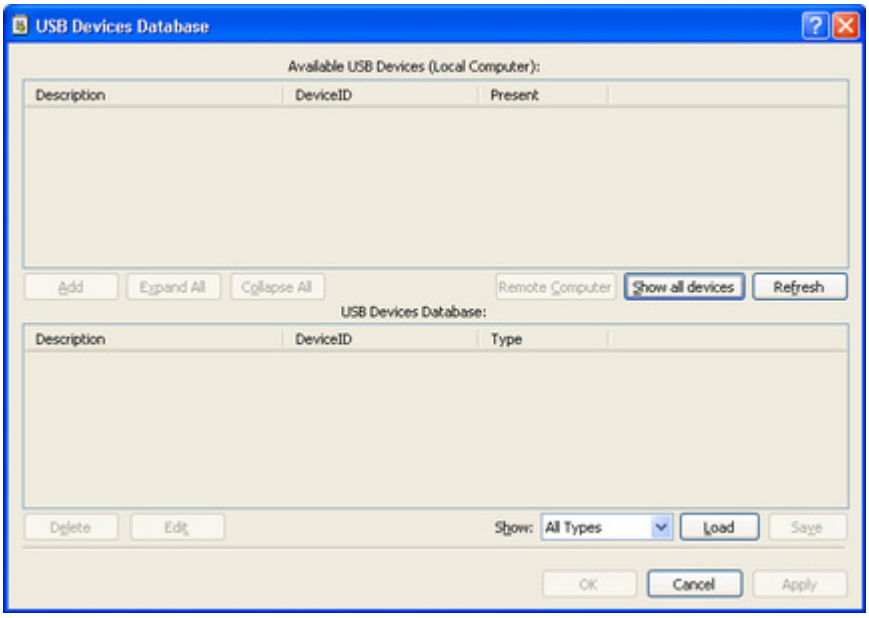
- Selezionare **USB Devices White List**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo USB Devices White List (Offline).



4. Nel riquadro superiore della finestra di dialogo **USB Devices White List (Offline)**, sotto **USB Devices Database**, fare clic su **USB Devices Database**.

   Viene visualizzata la finestra di dialogo USB Devices Database.



Nel riquadro superiore della finestra di dialogo USB Devices Database, sotto Available USB Devices, vengono visualizzate le periferiche correntemente collegate.

Per visualizzare la cronologia di tutte le periferiche collegate alle porte USB del computer, fare clic su **Show all devices**. Per visualizzare le periferiche disponibili su un computer remoto, fare clic su **Remote Computer**.

Il pulsante Remote Computer non è disponibile se la console di gestione è collegata al computer locale.

5. Nel riquadro superiore della finestra di dialogo **USB Devices Database**, sotto **Available USB Devices**, selezionare la periferica da aggiungere alla lista bianca delle periferiche USB e fare clic su **Add**.

   La periferica aggiunta viene visualizzata sotto USB Devices Database (Database delle periferiche USB), nel riquadro inferiore della finestra di dialogo.

   Nota: è possibile aggiungere una periferica alla lista bianca delle periferiche USB solo dopo averla aggiunta nel database delle periferiche USB.

   Lo stesso database viene usato per la lista bianca delle periferiche USB online e per quella offline.

   Per eliminare una periferica dal database delle periferiche USB, nel riquadro inferiore della finestra di dialogo **USB Devices Database**, sotto **USB Devices Database**, eseguire una delle seguenti azioni:

   - Selezionare la periferica e scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse sulla periferica, quindi scegliere **Delete**.

   Dopo essere state eliminate dal database delle periferiche USB, queste ultime non vengono eliminate automaticamente dalla lista bianca.

   Per modificare la descrizione di una periferica, nel riquadro inferiore della finestra di dialogo **USB Devices Database**, sotto **USB Devices Database**, selezionare la periferica e fare clic su **Edit**.

   Se si modifica la descrizione di una periferica nel database USB, all'interno della lista bianca la periferica manterrà la descrizione precedente, se è già stata aggiunta nella lista.

6. Fare clic su **OK** o su **Apply**.

   La periferica aggiunta nel database delle periferiche USB viene visualizzata sotto USB Devices Database, nel riquadro superiore della finestra di dialogo USB Devices White List (Offline).

7. Nel riquadro inferiore sinistro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

8. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la lista bianca delle periferiche USB, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo USB Devices White List (Offline).

Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

9. Nel riquadro inferiore sinistro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

10. Nel riquadro superiore della finestra di dialogo **USB Devices White List (Offline)**, sotto **USB Devices Database**, selezionare la periferica da aggiungere alla lista bianca per l'utente o gruppo selezionato, quindi fare clic su **Add**.

    È possibile selezionare più periferiche tenendo premuto il tasto MAIUSC o CTRL e facendo clic sulle periferiche.

    Le periferiche aggiunte nella lista bianca vengono visualizzate sotto Devices, nel riquadro inferiore destro della finestra di dialogo.

    Per eliminare una periferica dalla lista bianca per l'utente o gruppo selezionato, nel riquadro inferiore destro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Devices**, attenersi alle seguenti istruzioni:

    - Selezionare la periferica e scegliere **Delete**.
      - OPPURE -
    - Fare clic con il pulsante destro del mouse sulla periferica, quindi scegliere **Delete**.
      - OPPURE -
    - Selezionare la periferica e premere il tasto CANC.

    Per modificare la descrizione di una periferica, nel riquadro inferiore destro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Devices**, attenersi alle seguenti istruzioni:

    - Selezionare la periferica e fare clic su **Edit**.
      - OPPURE -
    - Fare clic con il pulsante destro del mouse sulla periferica, quindi scegliere **Edit**.

11. Fare clic su **OK** o su **Apply**.

Esportazione e importazione della lista bianca delle periferiche USB offline

È possibile esportare la USB Device White List (Lista bianca delle periferiche USB) offline in un file .whl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare la lista bianca delle periferiche USB offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Save Offline**.
     - OPPURE -
   - Selezionare **USB Devices White List**, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **USB Devices White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save Offline**.
     - OPPURE -
   - Espandere **USB Devices White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla periferica inclusa nella lista, quindi scegliere **Save**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Devices**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .whl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   La lista bianca delle periferiche USB offline esportata viene salvata in un file con estensione .whl.

Come importare la lista bianca delle periferiche USB offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Load Offline**.
     - OPPURE -
   - Selezionare **USB Devices White List**, quindi fare clic su **Load Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **USB Devices White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load Offline**.
     - OPPURE -
   - Espandere **USB Devices White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla periferica inclusa nella lista, quindi scegliere **Load**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **USB Devices White List (Offline)**, sotto **Devices**, fare clic su **Load**.

   Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open,** nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

Rimozione della definizione della lista bianca delle periferiche USB offline

È possibile riportare la lista bianca offline precedentemente definita allo stato non configurato. Se la lista bianca offline non è definita, ai computer client offline viene applicata la lista bianca Regular (normale).

Come rimuovere la definizione della lista bianca delle periferiche USB offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Undefine Offline**.

   Lo stato offline della lista bianca cambia in "Not Configured" (Non configurato).

   Selezionando **USB Devices White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline USB White List is not configured" (La lista bianca USB offline non è configurata).

Rimozione della lista bianca delle periferiche USB offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità della lista bianca offline di livello superiore e applicare la lista bianca normale a specifici gruppi di computer client di livello inferiore. Per applicare la lista bianca delle periferiche USB normale, occorre rimuovere le lista bianca delle periferiche USB offline.

Come rimuovere la lista bianca delle periferiche USB offline

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **USB Devices White List**, quindi scegliere **Remove Offline**.

   Lo stato offline della lista bianca cambia in "Use Regular" (Usa normale).

   Selezionando **USB Devices White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline USB White List is configured to use Regular USB White List" (La lista bianca USB offline è configurata per l'utilizzo della lista bianca USB normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione della lista bianca delle unità offline

Per una descrizione dettagliata della funzione Media White List (Lista bianca unità), consultare la sezione "Media White List (Regular Profile)".

La lista bianca delle unità offline può presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che la lista bianca non è definita. Viene visualizzato il messaggio "Offline Media List is not configured" (La lista bianca delle unità offline non è configurata). Si tratta dello stato predefinito.
Configured	Indica che la lista bianca è definita.
Use Regular	Indica che l'eredità della lista bianca offline è bloccata ed è applicata la lista bianca Regular (normale). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione della lista bianca normale è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione della lista bianca normale consente di evitare che la lista bianca offline ereditata da un livello superiore venga applicata a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione della lista bianca normale, consultare la sezione "Rimozione della lista bianca delle unità offline".

La gestione della lista bianca delle unità offline include le seguenti attività:

- Definizione e modifica della lista bianca delle unità offline
- Esportazione e importazione della lista bianca delle unità offline
- Rimozione della definizione della lista bianca delle unità offline
- Rimozione della lista bianca delle unità offline

Definizione e modifica della lista bianca delle unità offline

Come definire e modificare la lista bianca delle unità offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

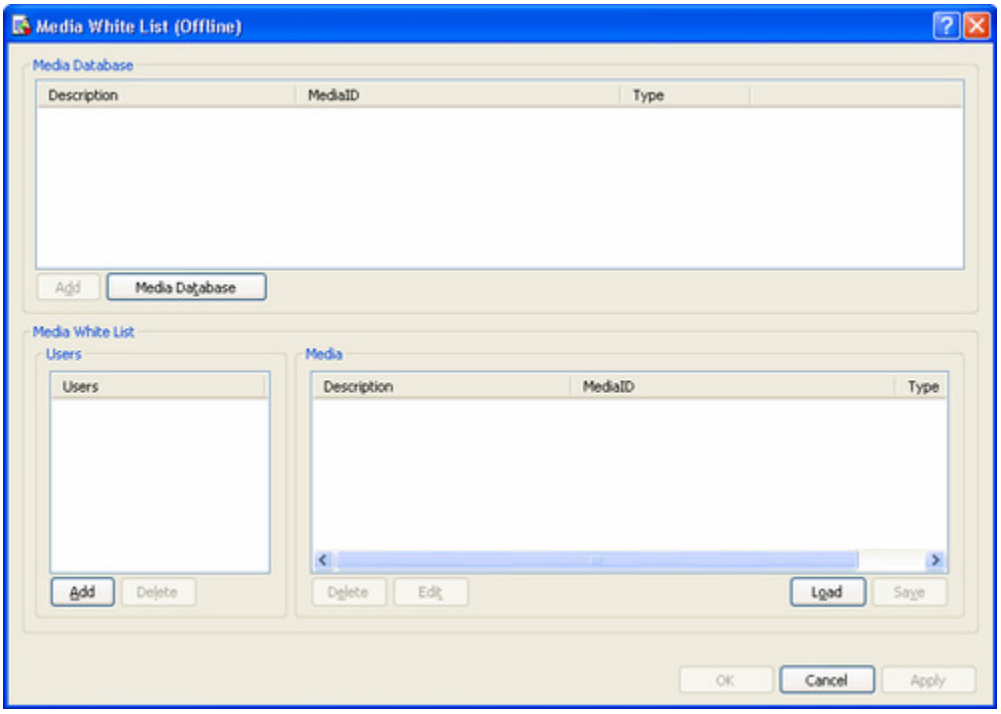
   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Manage Offline**.

- OPPURE -

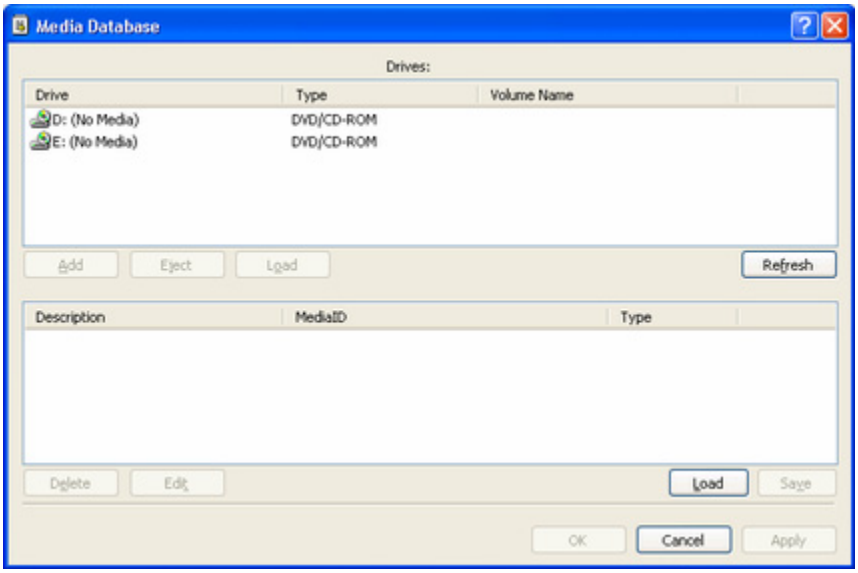
- Selezionare **Media White List**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Media White List (Offline).



4. Nel riquadro superiore della finestra di dialogo **Media White List (Offline)**, sotto **Media Database**, fare clic su **Media Database**.

   Viene visualizzata la finestra di dialogo Media Database.



Nel riquadro superiore della finestra di dialogo Media Database, sotto Drives, vengono visualizzate tutte le unità CD-ROM e DVD-ROM disponibili sul computer locale.

*L'elenco delle unità viene aggiornato automaticamente e le nuove unità sono visualizzate non appena vengono aggiunte. Per aggiornare manualmente l'elenco, fare clic su **Refresh**.*

5. Nel riquadro superiore della finestra di dialogo **Media Database**, sotto **Drives**, selezionare l'unità da aggiungere alla lista bianca delle unità e fare clic su **Add**.

   L'unità selezionata viene aggiunta al Media Database (Database delle unità) e può essere visualizzata nel riquadro inferiore della finestra di dialogo Media Database.

   Nota: è possibile aggiungere un'unità alla lista bianca delle unità solo dopo averla aggiunta nel database delle unità.

   Lo stesso database viene usato per la lista bianca delle unità online e per quella offline.

   Per eliminare un'unità dal database delle unità, nel riquadro inferiore della finestra di dialogo **Media Database**, attenersi alle seguenti istruzioni:

   - Selezionare l'unità e scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse sull'unità, quindi scegliere **Delete**.

   Per modificare la descrizione di un'unità, nel riquadro inferiore della finestra di dialogo **Media Database**, selezionare l'unità e fare clic su **Edit**.

6. Fare clic su **OK** o su **Apply**.

   L'unità aggiunta nel database delle unità viene visualizzata sotto Media Database, nel riquadro superiore della finestra di dialogo Media White List (Offline).

7. Nel riquadro inferiore sinistro della finestra di dialogo **Media White List (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

8. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la lista bianca delle unità, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Media White List (Offline).

   Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **Media White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

9. Nel riquadro inferiore sinistro della finestra di dialogo **Media White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

10. Nel riquadro superiore della finestra di dialogo **Media White List (Offline)**, sotto **Media Database**, selezionare l'unità da aggiungere alla lista bianca per l'utente o gruppo selezionato, quindi fare clic su **Add**.

È possibile selezionare più unità tenendo premuto il tasto MAIUSC o CTRL e facendo clic sulle unità.

Le unità aggiunte nella lista bianca vengono visualizzate sotto Media, nel riquadro inferiore destro della finestra di dialogo.

Per eliminare un'unità dalla lista bianca per l'utente o gruppo selezionato, nel riquadro inferiore destro della finestra di dialogo **Media White List (Offline)**, sotto **Media**, attenersi alle seguenti istruzioni:

- Selezionare l'unità e scegliere **Delete**.
  - OPPURE -
- Fare clic con il pulsante destro del mouse sull'unità, quindi scegliere **Delete**.

Per modificare la descrizione di un'unità, nel riquadro inferiore destro della finestra di dialogo **Media White List (Offline)**, sotto **Media**, attenersi alle seguenti istruzioni:

- Selezionare l'unità e fare clic su **Edit**.
  - OPPURE -
- Fare clic con il pulsante destro del mouse sull'unità, quindi scegliere **Edit**.

11. Fare clic su **OK** o su **Apply**.

Esportazione e importazione della lista bianca delle unità offline

È possibile esportare la Media White List (Lista bianca delle unità) offline in un file .mwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare la lista bianca delle unità

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Save Offline**.
     - OPPURE -
   - Selezionare **Media White List**, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -

- Espandere **Media White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save Offline**.

  - OPPURE -

- Espandere **Media White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sull'unità inclusa nella lista, quindi scegliere **Save**.

  - OPPURE -

- Fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Media White List (Offline)**, sotto **Media**, fare clic su **Save**.

Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .mwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   La lista bianca delle unità offline esportata viene salvata in un file con estensione .whl.

Come importare la lista bianca delle unità

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Load Offline**.

     - OPPURE -

   - Selezionare **Media White List**, quindi fare clic su **Load Offline** sulla barra degli strumenti.

     - OPPURE -

   - Espandere **Media White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load Offline**.

     - OPPURE -

- Espandere **Media White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla periferica inclusa nella lista, quindi scegliere **Load**.

  - OPPURE -

- Fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Media White List (Offline)**, sotto **Media**, fare clic su **Load**.

Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

Rimozione della definizione della lista bianca delle unità offline

È possibile riportare la lista bianca offline precedentemente definita allo stato non configurato. Se la lista bianca offline non è definita, ai computer client offline viene applicata la lista bianca Regular (normale).

Come rimuovere la definizione della lista bianca delle unità offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Undefine Offline**.

   Lo stato offline della lista bianca cambia in "Not Configured" (Non configurato).

   Selezionando **Media White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Media White List is not configured" (La lista bianca delle unità offline non è configurata).

Rimozione della lista bianca delle unità offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità della lista bianca offline di

livello superiore e applicare la lista bianca normale a specifici gruppi di computer client di livello inferiore. Per applicare la lista bianca delle unità normale, occorre rimuovere le lista bianca delle unità offline.

Come rimuovere la lista bianca delle unità offline

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Media White List**, quindi scegliere **Remove Offline**.

   Lo stato offline della lista bianca cambia in "Use Regular" (Usa normale).

   Selezionando **Media White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Media White List is configured to use Regular Media White List" (La lista bianca delle unità offline è configurata per l'utilizzo della lista bianca delle unità normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle regole basate sul contenuto offline per le periferiche

Per una descrizione dettagliata della funzione Content-Aware Rules (Regole basate sul contenuto) per le periferiche, consultare la sezione "Regole basate sul contenuto per le periferiche (Regular Profile)".

Le regole basate sul contenuto possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le regole basate sul contenuto non sono definite. Viene visualizzato il messaggio "Offline Content-Aware Rules are not configured" (Le regole basate sul contenuto offline non sono configurate). Si tratta dello stato predefinito.
Configured	Indica che le regole basate sul contenuto sono definite.

STATO	DESCRIZIONE
Use Regular	Indica che l'eredità delle regole basate sul contenuto offline è bloccata e sono applicate le regole basate sul contenuto Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle regole basate sul contenuto normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle regole basate sul contenuto normali consente di evitare che le regole basate sul contenuto offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle regole basate sul contenuto normali, consultare la sezione "Rimozione delle regole basate sul contenuto offline".

La gestione delle regole basate sul contenuto offline include le seguenti attività:

- Definizione delle regole basate sul contenuto offline
- Modifica delle regole basate sul contenuto offline
- Copia delle regole basate sul contenuto offline
- Esportazione e importazione delle regole basate sul contenuto offline
- Eliminazione delle regole basate sul contenuto offline
- Rimozione della definizione delle regole basate sul contenuto offline
- Rimozione delle regole basate sul contenuto offline

Definizione delle regole basate sul contenuto offline

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto incorporati o personalizzati. Per informazioni dettagliate su questi gruppi, consultare la sezione "Configurazione delle impostazioni di rilevamento del contenuto".

Per definire una regola basata sul contenuto (Content-Aware Rule) offline

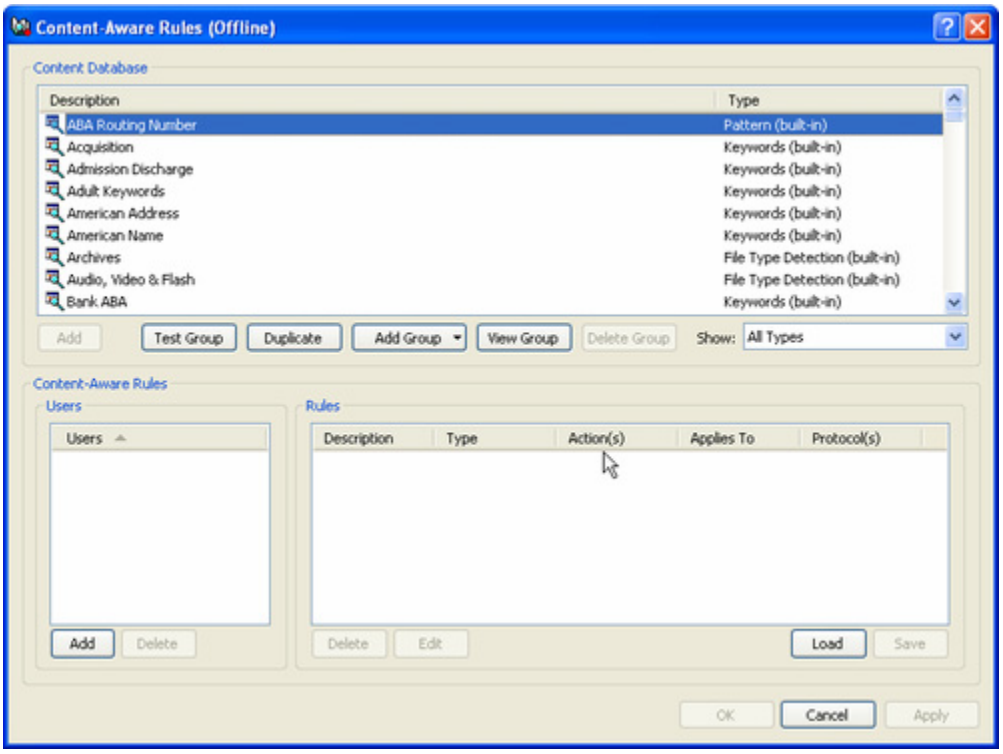
1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules (Offline).



4. I Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la regola, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules (Offline).

   Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

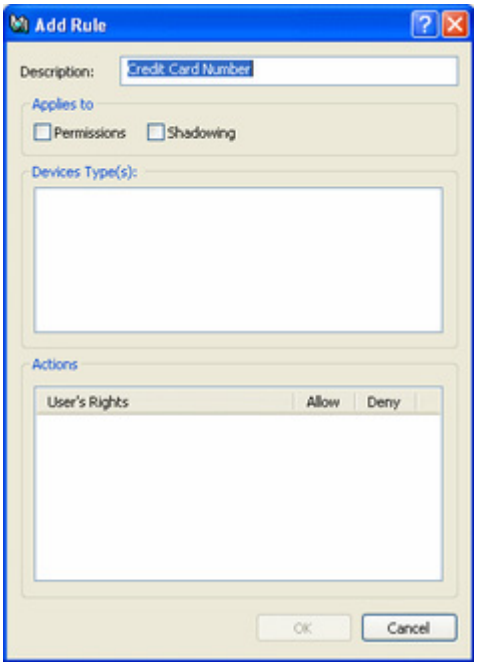
6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare gli utenti o i gruppi per cui si desidera definire la regola.

È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

7. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **Add**.

   Nota: è possibile specificare un solo gruppo di contenuto per ogni regola basata sul contenuto.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, nella casella **Description**, digitare il nome della regola basata sul contenuto.

   Per impostazione predefinita, quest'ultima ha lo stesso nome del gruppo di contenuto specificato, ma è possibile specificare un altro nome.

9. Sotto **Applies to**, specificare il tipo di operazione associata con la regola. Le opzioni disponibili sono:

   - **Permissions**: specifica che la regola verrà applicata alle operazioni di controllo dell'accesso.
   - **Shadowing**: specifica che la regola verrà applicata alle operazioni di copia shadow.
   - **Permissions**, **Shadowing**: specifica che la regola verrà applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.

10. Sotto **Device Type(s)**, selezionare i tipi di periferica appropriati a cui si desidera applicare la regola.

    Le regole basate sul contenuto possono essere applicate ai tipi di periferica DVD/CD-ROM, Floppy, iPhone, Palm, Removable e Windows Mobile.

11. Sotto **Action(s)**, specificare quali azioni degli utenti sono autorizzate o non autorizzate per i file e quali azioni degli utenti vanno inserite nel registro shadowing.

    È possibile selezionare una qualsiasi delle seguenti opzioni: Read (lettura), Write (scrittura) e Read and Write (lettura e scrittura).

    Se la regola viene applicata alle operazioni di copia shadow o sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow, l'opzione Read non è disponibile. Per informazioni dettagliate sui diritti degli utenti che possono essere specificati nelle regole basate sui contenuti, consultare le sezioni "Regole basate sul contenuto per le operazioni di controllo dell'accesso" e "Regole basate sul contenuto per le operazioni di copia shadow".

12. Fare clic su **OK**.

    La regola creata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules (Offline).

13. Fare clic su **OK** o su **Apply** per applicare la regola.

    Gli utenti o i gruppi per cui è stata applicata la regola basata sul contenuto vengono visualizzati sotto Content-Aware Rules nella struttura della console.

    Se nella struttura della console viene selezionato un utente o un gruppo per cui è stata applicata una regola basata sul contenuto, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:

    - **Description** Il nome della regola. Per impostazione predefinita, la regola ha lo stesso nome del gruppo di contenuto specificato.
    - **Type** Il tipo di analisi del contenuto. Valori possibili: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties** e **Complex**. **File Type Detection** indica che il riconoscimento e l'identificazione dei file si basa sulle loro firme caratteristiche. **Keywords** indica che il riconoscimento e l'identificazione dei file/dati si basa sulle parole chiave o frasi specificate. **Pattern** indica che il riconoscimento e l'identificazione dei file/dati si basa sui motivi di testo specificati descritti dalle espressioni comuni Perl. **Document Properties** indica che il riconoscimento e l'identificazione dei file si basa sulle loro proprietà. **Complex** indica che il riconoscimento e l'identificazione dei file/dati si basa sul contenuto specificato descritto da un'espressione booleana.
    - **Action(s)** Mostra quali azioni degli utenti sono autorizzate o non autorizzate per i file e quali azioni degli utenti vanno inserite nel registro shadowing.
    - **Applies To** Valori possibili: **Permissions**, **Shadowing**, e **Permissions, Shadowing**. **Permissions** indica che la regola viene applicata alle operazioni di controllo dell'accesso. **Shadowing** indica che la regola viene applicata alle operazioni di copia shadow. **Permissions, Shadowing** indica che la regola viene applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.
    - **Device Type(s)** Il tipo (o i tipi) di dispositivo per cui viene applicata la regola.
    - **Profile** Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

      È possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire le

regole basate sul contenuto online, consultare la sezione "Gestione delle regole basate sul contenuto".

Modifica delle regole basate sul contenuto offline

È possibile modificare le proprietà delle Content-Aware Rules (regole basate sul contenuto) come Description, Applies To, Device Type(s) e Actions (Descrizione, Si applica a, Tipi di periferica e Azioni).

Come modificare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto Devices, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, scegliere **Manage Offline**, quindi attenersi alla procedura seguente:
   a) Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.
   b) Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.
   - OPPURE -
   Fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Edit**.

   - OPPURE -

   Sotto **Devices**, espandere **Content-Aware Rules**, quindi attenersi alla procedura seguente:
   a) Sotto **Content-Aware Rules**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto applicati agli stessi nel riquadro dei dettagli.
   b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.

   Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare le proprietà della regola a seconda delle proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole basate sul contenuto offline

Per riutilizzare le Content-Aware Rules (regole basate sul contenuto) offline esistenti, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Come copiare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules (Offline).
4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.
5. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. In caso di taglio, la regola viene eliminata solo dopo essere stata incollata.

Per eseguire un'operazione di trascinamento, selezionare la regola e spostarla verso l'utente o il gruppo a cui si desidera applicare la regola copiata.

6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi a cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules (Offline).

8. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare gli utenti o i gruppi per cui si desidera impostare le autorizzazioni.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

9. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, fare clic con il pulsante destro del mouse sul riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules (Offline).

10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione delle regole basate sul contenuto offline

È possibile esportare tutte le Content-Aware Rules (regole basate sul contenuto) offline correnti in un file .cwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.

3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Save Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo, quindi scegliere **Save Offline**.
     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .cwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   Le regole esportate vengono salvate in un file con estensione .cwl.

Come importare le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Load Offline**.
  - OPPURE -
- Selezionare **Content-Aware Rules**, quindi fare clic su **Load Offline** sulla barra degli strumenti.
  - OPPURE -
- Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo, quindi scegliere **Load Offline**.
  - OPPURE -
- Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Load**.
  - OPPURE -
- Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Load Offline** sulla barra degli strumenti.
  - OPPURE -
- Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic su **Load**.

Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   È possibile importare un solo file .cwl alla volta.

Eliminazione delle regole basate sul contenuto offline

Quando alcune Content-Aware Rules (regole basate sul contenuto) offline non sono più necessarie, possono essere eliminate.

Come eliminare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo a cui viene applicata la regola, quindi scegliere **Delete user**.
     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.

     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.
     È possibile selezionare più regole da eliminare tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sulle regole.

Rimozione della definizione delle regole basate sul contenuto offline

È possibile riportare le regole basate sul contenuto offline precedentemente definite al loro stato non configurato. Se le regole offline non sono definite, ai computer client offline vengono applicate le regole normali.

Come rimuovere la definizione delle regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Undefine Offline**.

   Lo stato offline delle regole basate sul contenuto cambia in "Not Configured" (Non configurato).

Selezionando **Content-Aware Rules** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Content-Aware Rules are not configured" (Le regole basate sul contenuto offline non sono configurate).

Rimozione delle regole basate sul contenuto offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle regole basate sul contenuto offline di livello superiore e applicare le regole basate sul contenuto normali a specifici gruppi di computer client di livello inferiore. Per applicare le regole basate sul contenuto Regular (normali), occorre rimuovere le regole basate sul contenuto offline.

Come rimuovere le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Remove Offline**.

   Lo stato offline delle regole basate sul contenuto cambia in "Use Regular" (Usa normale).

   Selezionando **Content-Aware Rules** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules" (Le regole basate sul contenuto offline sono configurate per l'utilizzo delle regole basate sul contenuto normali).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle impostazioni di protezione offline

Per una descrizione dettagliata della funzione Security Settings (Impostazioni di protezione), consultare la sezione "Security Settings (Regular Profile)".

Le impostazioni di protezione offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le impostazioni di protezione offline non sono definite. Si tratta dello stato predefinito.
Enabled	Indica che le impostazioni di protezione offline sono definite per abilitare il controllo dell'accesso per le classi di periferiche specificate.

STATO	DESCRIZIONE
Disabled	Indica che le impostazioni di protezione offline sono definite per disabilitare il controllo dell'accesso per le classi di periferiche specificate.
Use Regular	Indica che l'eredità delle impostazioni di protezione offline è bloccata e sono applicate le impostazioni di protezione Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle impostazioni di protezione normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle impostazioni di protezione normali consente di evitare che le impostazioni di protezione offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle impostazioni di protezione normali, consultare la sezione "Rimozione delle impostazioni di protezione offline".

La gestione delle impostazioni di protezione offline prevede le seguenti attività:

- Definizione e modifica delle impostazioni di protezione offline
- Rimozione della definizione delle impostazioni di protezione offline
- Rimozione delle impostazioni di protezione offline

Definizione e modifica delle impostazioni di protezione offline

Le Security Settings (impostazioni di protezione) offline) possono essere modificate singolarmente o in gruppo.

Come definire e modificare singole impostazioni di protezione offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Security Settings**.

   Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione, quindi scegliere **Enable Offline**.

   Lo stato offline dell'impostazione di protezione cambia da "Not Configured" (Non configurato) a "Enabled" (Abilitato).

   Dopo aver abilitato un'impostazione di sicurezza, è possibile disabilitarla. Per farlo, fare clic con il pulsante destro del mouse sull'impostazione di sicurezza abilitata, quindi scegliere **Disable Offline**.

   Lo stato offline dell'impostazione di protezione cambia da "Enabled" (Abilitato) a "Disabled" (Disabilitato).

Come definire e modificare più impostazioni di protezione offline

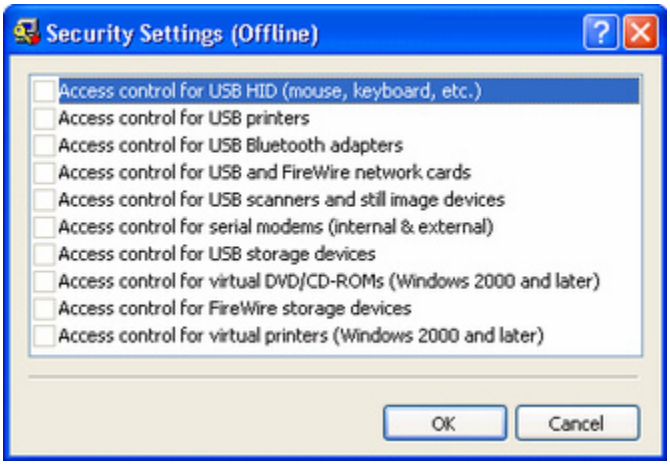
1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Security Settings**, quindi scegliere **Manage Offline**.
     - OPPURE –
   - Selezionare **Security Settings**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.
     - OPPURE -
   - Selezionare **Security Settings**. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione, quindi scegliere **Manage Offline.**
     - OPPURE –
   - Selezionare **Security Settings**. Nel riquadro dei dettagli, selezionare una qualsiasi impostazione di sicurezza, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

     Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

   Viene visualizzata la finestra di dialogo Security Settings (Offline).


Security Settings (Offline)
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB Bluetooth adapters
Access control for USB and FireWire network cards
Access control for USB scanners and still image devices
Access control for serial modems (internal & external)
Access control for USB storage devices
Access control for virtual DVD/CD-ROMs (Windows 2000 and later)
Access control for FireWire storage devices
Access control for virtual printers (Windows 2000 and later)
OK
Cancel

4. Nella finestra di dialogo **Security Settings (Offline)**, selezionare le caselle di controllo relative alle impostazioni di protezione da definire.

   Dopo aver abilitato le impostazioni di sicurezza, è possibile disabilitarle. Per farlo, deselezionare le caselle di controllo pertinenti.

   Nota: tutte le caselle di controllo della finestra di dialogo **Security Settings (Offline)** presentano tre stati: selezionato, deselezionato e indeterminato, corrispondenti agli stati Enabled (Abilitato), Disabled (Disabilitato) e Not Configured (Non configurato) delle impostazioni di protezione.

5. Fare clic su **OK**.

Rimozione della definizione delle impostazioni di protezione offline

È possibile riportare le impostazioni di protezione precedentemente definite allo stato non configurato. Se le impostazioni di protezione offline non sono definite, ai computer client offline vengono applicate le impostazioni di protezione normali. È possibile rimuovere la definizione delle impostazioni di protezione singolarmente o in gruppo.

Come rimuovere la definizione di singole impostazioni di protezione offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Security Settings**.

Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione per cui si desidera rimuovere la definizione, quindi scegliere **Undefine Offline**.

   Lo stato offline dell'impostazione di protezione cambia in "Not Configured" (Non configurato).

Come rimuovere la definizione di più impostazioni di protezione offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Security Settings**, quindi scegliere **Manage Offline**.
     - OPPURE –
   - Selezionare **Security Settings**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.
     - OPPURE -
   - Selezionare **Security Settings**. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione, quindi scegliere **Manage Offline.**
     - OPPURE –
   - Selezionare **Security Settings**. Nel riquadro dei dettagli, selezionare una qualsiasi impostazione di sicurezza, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

     Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

   Viene visualizzata la finestra di dialogo Security Settings (Offline).

4. Nella finestra di dialogo **Security Settings (Offline)**, impostare nuovamente le caselle di controllo appropriate sullo stato indeterminato.

Nota: tutte le caselle di controllo della finestra di dialogo **Security Settings (Offline)** presentano tre stati: selezionato, deselezionato e indeterminato, corrispondenti agli stati

Enabled (Abilitato), Disabled (Disabilitato) e Not Configured (Non configurato) delle impostazioni di protezione.

Rimozione delle impostazioni di protezione offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle impostazioni di protezione offline di livello superiore e applicare le impostazioni di protezione normali a specifici gruppi di computer client di livello inferiore. Per applicare le impostazioni di protezione normali, occorre rimuovere le impostazioni di protezione offline. Le impostazioni di protezione possono essere rimosse solo singolarmente.

Come rimuovere le impostazioni di protezione offline

1. Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Devices**.
3. Sotto **Devices**, selezionare **Security Settings**.

   Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione da rimuovere, quindi scegliere **Remove Offline**.

   Lo stato offline delle impostazioni di protezione cambia in "Use Regular" (Usa normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione dei criteri di protezione offline per i protocolli

La gestione dei criteri di protezione offline per i protocolli prevede le seguenti operazioni:

- Gestione delle autorizzazioni offline per i protocolli
- Gestione delle regole di controllo e shadowing offline per i protocolli
- Gestione della lista bianca dei protocolli offline
- Gestione delle regole basate sul contenuto offline per i protocolli
- Gestione delle impostazioni di protezione offline per i protocolli

Gestione delle autorizzazioni offline per i protocolli

Per una descrizione dettagliata della funzione Permissions (Autorizzazioni) per i protocolli, consultare la sezione "Gestione delle autorizzazioni per i protocolli".

Le autorizzazioni offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le autorizzazioni per un protocollo non sono state configurate. Si tratta dello stato predefinito.
Configured	Indica che le autorizzazioni per un protocollo sono state configurate.
Full Access	Indica che i diritti di accesso completi sono concessi all'account Everyone.
No Access	Indica una delle seguenti condizioni: • L'account Everyone dispone delle autorizzazioni di tipo No Access ed è l'unico account assegnato a un protocollo. *Le autorizzazioni No Access assegnate all'account Everyone hanno la priorità sulle autorizzazioni assegnate agli altri account.* • Tutti gli utenti e i gruppi assegnati a un protocollo hanno le autorizzazioni di tipo No Access. • Tutti gli utenti e i gruppi assegnati a un protocollo sono stati rimossi.
Use Regular	Indica che l'eredità delle autorizzazioni offline è bloccata e sono applicate le autorizzazioni Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle autorizzazioni normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle autorizzazioni normali consente di evitare che le autorizzazioni offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle autorizzazioni normali, consultare la sezione "Rimozione delle autorizzazioni offline".

La gestione delle autorizzazioni offline include le seguenti attività:

- Impostazione e modifica delle autorizzazioni offline
- Rimozione della definizione delle autorizzazioni offline
- Rimozione delle autorizzazioni offline

Impostazione e modifica delle autorizzazioni offline

Come impostare e modificare le autorizzazioni offline

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

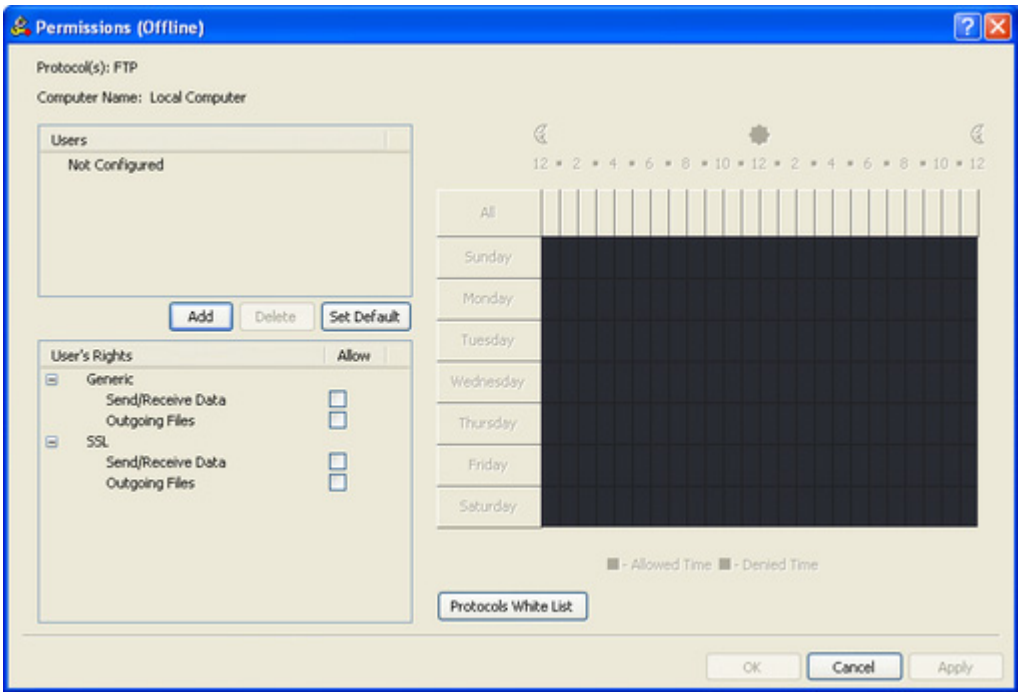
Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Permissions**.

   Dopo aver selezionato Permissions nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun protocollo.
4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse sul protocollo per cui si desidera impostare o modificare le autorizzazioni, quindi scegliere **Set Offline Permissions**.
     - OPPURE -
   - Selezionare il protocollo per cui si desidera impostare o modificare le autorizzazioni, quindi fare clic su **Set Offline Permissions** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Permissions (Offline).



5. Nella finestra di dialogo **Permissions (Offline)**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Impostare le autorizzazioni predefinite	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**. *Le autorizzazioni predefinite sono assegnate agli account Administrators ed Everyone. Per informazioni sulle autorizzazioni assegnate a questi account per impostazione predefinita, consultare la sezione* "Gestione delle autorizzazioni per i protocolli".
Impostare le autorizzazioni per un ulteriore utente o gruppo	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 2. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Permissions (Offline).* 3. Nel riquadro superiore sinistro della finestra di dialogo **Permissions (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti e/o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi*. 4. Nel riquadro inferiore sinistro della finestra di dialogo **Permissions (Offline)**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati. *Nel riquadro destro della finestra di dialogo Permissions (Offline), è possibile impostare le restrizioni per data e ora, al fine di limitare l'accesso ai protocolli specificati da parte dell'utente. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui l'utente o il gruppo selezionato può accedere ai protocolli specificati. Utilizzare il pulsante destro del mouse per contrassegnare i giorni e le ore in cui l'utente o il gruppo selezionato non può accedere ai protocolli specificati*.
Modificare le autorizzazioni per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti di accesso appropriati.
Rimuovere un utente o gruppo esistente e le autorizzazioni	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle autorizzazioni offline

È possibile riportare le autorizzazioni offline precedentemente definite allo stato non configurato. Se le autorizzazioni non sono definite, ai computer client offline vengono applicate le autorizzazioni normali.

Come rimuovere la definizione delle autorizzazioni offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Permissions**.

   Dopo aver selezionato Permissions nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun protocollo.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere la definizione delle autorizzazioni offline, quindi selezionare **Undefine Offline**.

   È possibile rimuovere simultaneamente la definizione delle autorizzazioni offline impostate per più protocolli. Per farlo, attenersi alle seguenti istruzioni:
   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui protocolli.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine Offline**.

   Lo stato offline delle autorizzazioni cambia in "Not Configured" (Non configurato).

Rimozione delle autorizzazioni offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle autorizzazioni offline di livello superiore e applicare le autorizzazioni normali a specifici gruppi di computer client di livello inferiore. Per applicare le autorizzazioni normali, occorre rimuovere le autorizzazioni offline.

Come rimuovere le autorizzazioni offline

1. Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Permissions**.

   Dopo aver selezionato Permissions nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile impostare le autorizzazioni. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle autorizzazioni offline per ciascun protocollo.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere le autorizzazioni offline, quindi selezionare **Remove Offline**.

   È possibile rimuovere simultaneamente le autorizzazioni offline impostate per più protocolli. Per farlo, attenersi alle seguenti istruzioni:

   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sui protocolli.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Remove Offline**.

   Lo stato offline delle autorizzazioni cambia in "Use Regular" (Usa regolare).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle regole di controllo e shadowing offline per i protocolli

Per una descrizione dettagliata della funzione Auditing & Shadowing (Controllo e shadowing) per i protocolli, consultare la sezione "Gestione delle regole di controllo e shadowing per i protocolli".

Le regole di controllo e shadowing offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le regole di controllo e shadowing non sono state definite per un protocollo. Si tratta dello stato predefinito.
Configured	Indica che le regole di controllo e shadowing sono state definite per un protocollo.
No Audit	Indica una delle seguenti condizioni: • I diritti di Audit (Controllo) non sono stati impostati per tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un protocollo. • Tutti gli utenti e gruppi specificati nelle regole di controllo e shadowing per un protocollo sono stati rimossi. • L'account Everyone non dispone dei diritti Audit e Shadowing ed è l'unico

STATO	DESCRIZIONE
	account specificato nelle regole di controllo e shadowing per un protocollo.
Use Regular	Indica che l'eredità delle regole di controllo e shadowing offline è bloccata e sono applicate le regole di controllo e shadowing Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle regole normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle regole normali consente di evitare che le regole offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle regole normali, consultare la sezione "Rimozione delle regole di controllo e shadowing offline".

La gestione delle regole di controllo e shadowing offline include le seguenti attività:

- Definizione e modifica delle regole di controllo e shadowing offline
- Rimozione della definizione delle regole di controllo e shadowing offline
- Rimozione delle regole di controllo e shadowing offline

Definizione e modifica delle regole di controllo e shadowing offline

Come definire e modificare le regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Auditing & Shadowing**.

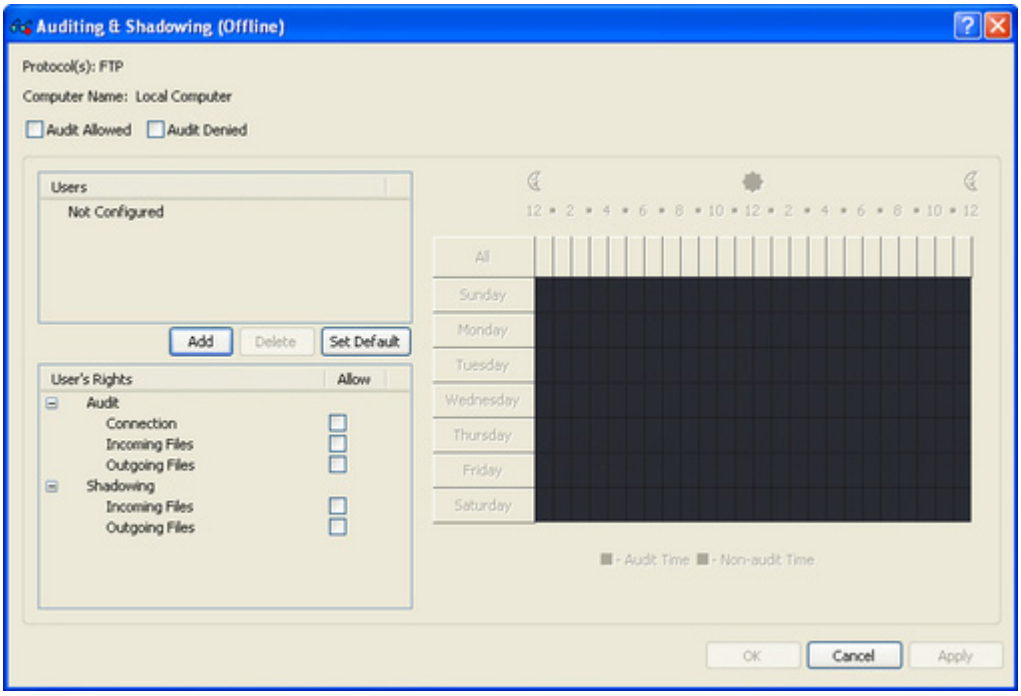
   Dopo aver selezionato Auditing & Shadowing nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun protocollo.
4. Nel riquadro dei dettagli, eseguire una delle seguenti azioni:

- Fare clic con il pulsante destro del mouse sul protocollo per cui si desidera definire o modificare le regole, quindi scegliere **Set Offline Auditing & Shadowing**.

  - OPPURE -

- Selezionare il protocollo per cui si desidera definire o modificare le regole, quindi fare clic su **Set Offline Auditing & Shadowing** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Auditing & Shadowing (Offline).



5. Nella finestra di dialogo **Auditing & Shadowing (Offline)**, attenersi alle seguenti istruzioni:

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
Definire le regole di controllo e shadowing predefinite	1. Nel riquadro superiore sinistro della finestra di dialogo, specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a un protocollo andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a un protocollo non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Set Default**. *Le regole di controllo e shadowing predefinite si applicano ai gruppi Users ed Everyone. Per informazioni sui diritti di controllo e shadowing impostati per questi account per impostazione predefinita, consultare la sezione "Gestione delle regole di controllo e shadowing per i protocolli".*
Definire le regole di	1. Nel riquadro superiore sinistro della finestra di dialogo,

PER ESEGUIRE QUESTA AZIONE	ESEGUIRE QUESTI PASSAGGI
controllo e shadowing per un ulteriore utente o gruppo	specificare gli eventi inseriti nel registro di controllo. Selezionare la casella di controllo **Audit Allowed** per controllare i tentativi di accesso a un protocollo andati a buon fine. Selezionare la casella di controllo **Audit Denied** per controllare i tentativi di accesso a un protocollo non andati a buon fine. 2. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, fare clic su **Add**. *Viene visualizzata la finestra di dialogo Select Users or Groups*. 3. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare il nome dell'utente o del gruppo, quindi fare clic su **OK**. *Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro superiore sinistro della finestra di dialogo Auditing & Shadowing (Offline).* 4. Nel riquadro superiore sinistro della finestra di dialogo **Auditing & Shadowing (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato. *È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi*. 5. Nel riquadro inferiore sinistro della finestra di dialogo **Auditing & Shadowing (Offline)**, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti appropriati. *Nel riquadro destro della finestra di dialogo Auditing & Shadowing (Offline), si possono specificare i giorni e le ore (ad esempio dalle 7 alle 17, dal lunedì al venerdì) in cui la regola per l'utente o il gruppo selezionato risulterà attiva o non attiva. Utilizzare il pulsante sinistro del mouse per selezionare i giorni e le ore in cui la regola sarà attiva (orario di controllo). Utilizzare il pulsante destro del mouse per contrassegnare i giorni e le ore in cui la regola non sarà attiva (orario senza controllo)*.
Modificare le regole di controllo e shadowing per un utente o gruppo esistente	1. Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo desiderato. 2. Nel riquadro inferiore sinistro della finestra di dialogo, sotto **User's Rights**, selezionare o deselezionare la casella di controllo **Allow** posta accanto ai diritti appropriati.
Rimuovere un utente o gruppo esistente e le regole associate	• Nel riquadro superiore sinistro della finestra di dialogo, sotto **Users**, selezionare l'utente o il gruppo, quindi fare clic su **Delete** o premere il tasto CANC. *Quando viene rimosso un utente o un gruppo, vengono rimosse anche tutte le regole associate a tale utente o gruppo*.

6. Fare clic su **OK** o su **Apply**.

Rimozione della definizione delle regole di controllo e shadowing offline

È possibile riportare le regole di controllo e shadowing offline precedentemente definite allo stato non configurato. Se le regole offline non sono definite, ai computer client offline vengono applicate le regole normali.

Come rimuovere la definizione delle regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun protocollo.
4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere la definizione delle regole di controllo e shadowing offline, quindi selezionare **Undefine Offline**.

   È possibile rimuovere simultaneamente la definizione delle regole di controllo e shadowing impostate per più protocolli. Per farlo, attenersi alle seguenti istruzioni:
   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui protocolli.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Undefine Offline**.

   Lo stato offline delle regole di controllo e shadowing cambia in "Not Configured" (Non configurato).

Rimozione delle regole di controllo e shadowing offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle regole di controllo e shadowing offline di livello superiore e applicare le regole di controllo e shadowing normali a specifici gruppi di computer client di livello inferiore. Per applicare le regole di controllo e shadowing Regular (normali), occorre rimuovere le regole di controllo e shadowing offline.

Come rimuovere le regole di controllo e shadowing offline

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Auditing & Shadowing**.

   Dopo aver selezionato Auditing & Shadowing nella struttura della console, nel riquadro dei dettagli vengono visualizzati i protocolli per cui è possibile definire le regole di controllo e shadowing. Nella colonna Offline del riquadro dei dettagli viene visualizzato lo stato corrente delle regole offline per ciascun protocollo.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sul protocollo per cui si desidera rimuovere le regole di controllo e shadowing offline, quindi selezionare **Remove Offline**.

   È possibile rimuovere simultaneamente le regole di controllo e shadowing definite per più protocolli. Per farlo, attenersi alle seguenti istruzioni:

   a) Nel riquadro dei dettagli, selezionare più protocolli tenendo premuto il tasto MAIUSC o CTRL e facendo clic sui protocolli.
   b) Fare clic con il pulsante destro del mouse sulla selezione e scegliere **Remove Offline**.

   Lo stato offline delle regole di controllo e shadowing cambia in "Use Regular" (Usa normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione della lista bianca dei protocolli offline

Per una descrizione dettagliata della funzione Protocols White List (Lista bianca protocolli), consultare la sezione "Gestione della lista bianca dei protocolli (Regular Profile)".

La lista bianca dei protocolli offline può presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che la lista bianca non è definita. Viene visualizzato il messaggio "Offline Protocols White List is not configured" (La lista bianca dei protocolli offline non è configurata). Si tratta dello stato predefinito.
Configured	Indica che la lista bianca è definita.
Use Regular	Indica che l'eredità della lista bianca offline è bloccata ed è applicata la lista bianca regolare. Viene visualizzato il seguente messaggio: "Offline Protocols White List is configured to use Regular Protocols White List" (La lista bianca dei

STATO	DESCRIZIONE
	protocolli offline è configurata per utilizzare la lista bianca dei protocolli regolare). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione della lista bianca regolare è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione della lista bianca regolare consente di evitare che la lista bianca offline ereditata da un livello superiore venga applicata a un gruppo specifico di computer client di livello inferiore. Per ulteriori informazioni sull'applicazione della lista bianca regolare, consultare la sezione "Rimozione della lista bianca dei protocolli offline".

La gestione della lista bianca dei protocolli offline include le seguenti attività:

- Definizione della lista bianca dei protocolli offline
- Modifica della lista bianca dei protocolli offline
- Copia delle regole della lista bianca dei protocolli offline
- Esportazione e importazione della lista bianca dei protocolli offline
- Eliminazione delle regole della lista bianca dei protocolli offline
- Rimozione della definizione della lista bianca dei protocolli offline
- Rimozione della lista bianca dei protocolli offline

Definizione della lista bianca dei protocolli offline

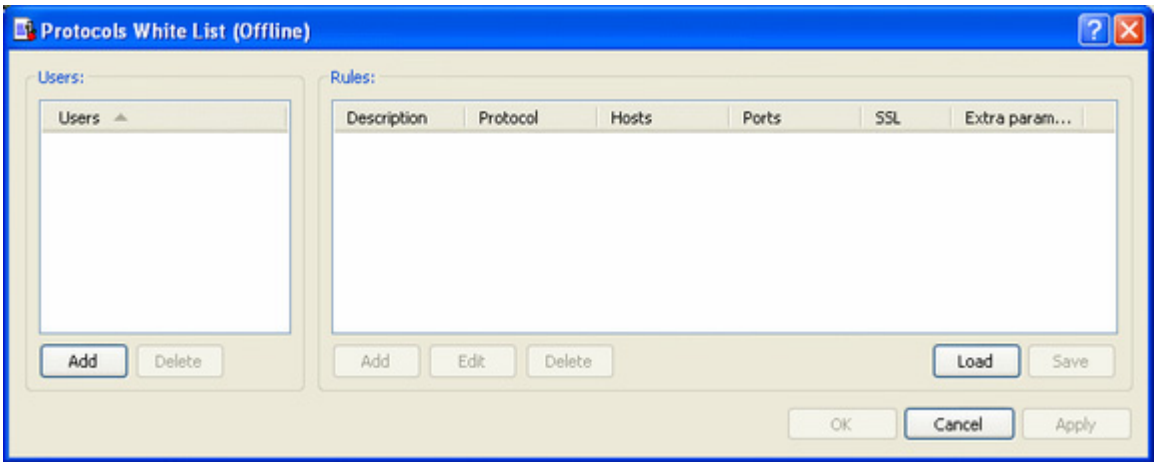
Per definire la lista bianca dei protocolli offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

Viene visualizzata la finestra di dialogo Protocols White List (Offline).



4. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la lista bianca dei protocolli, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro sinistro della finestra di dialogo Protocols White List (Offline).

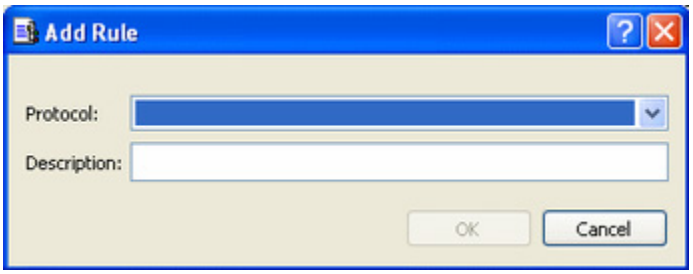
   Per eliminare un utente o un gruppo, nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** .

6. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi.

7. Nel riquadro destra della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, specificare i parametri generali e specifici per protocollo relativi a questa regola. Per specificare i parametri generali, attenersi alle seguenti istruzioni:

   - Per specificare il protocollo, selezionarlo nell'elenco **Protocol:**.

- Per specificare il nome della regola, digitarlo nella casella **Description**.

Per specificare i parametri specifici per protocollo, attenersi alle seguenti istruzioni:

- Per specificare gli host, digitare i nomi di host o gli indirizzi IP separati da una virgola o da un punto e virgola nella casella **Hosts:**. Per ulteriori informazioni su come specificare gli host, consultare la descrizione del parametro Hosts.
- Per specificare le porte, digitare i numeri di porta separati da una virgola o da un punto e virgola nella casella **Ports:**. Per ulteriori informazioni su come specificare le porte, consultare la descrizione del parametro Ports.
- Per configurare le opzioni SSL, sotto **SSL**, fare clic su una delle seguenti opzioni: **Allowed** (autorizza le connessioni SSL), **Denied** (nega le connessioni SSL) o **Required** (richiede l'utilizzo di SSL da parte di tutte le connessioni).
- Per specificare gli ID dei mittenti locali di messaggistica immediata, digitare gli ID utente separati da una virgola o da un punto e virgola nella casella **Local sender ID(s):**. Per ulteriori informazioni su come specificare gli ID utente, consultare la descrizione del parametro Local sender ID(s).
- Per specificare gli ID dei destinatari locali di messaggistica immediata, digitare gli ID utente separati da una virgola o da un punto e virgola nella casella **Remote recipient ID(s):**. Per ulteriori informazioni su come specificare gli ID utente, consultare la descrizione del parametro Remote recipient ID(s).
- Per specificare i mittenti di e-mail, digitare gli indirizzi dei mittenti separati da una virgola o da un punto e virgola nella casella **Local sender Email(s):**. Per ulteriori informazioni su come specificare gli indirizzi dei mittenti, consultare la descrizione del parametro Local sender Email(s):.
- Per specificare i destinatari di e-mail, digitare gli indirizzi dei destinatari separati da una virgola o da un punto e virgola nella casella **Remote recipient Email(s):**. Per ulteriori informazioni su come specificare gli indirizzi dei destinatari, consultare la descrizione del parametro Remote recipient Email(s):.
- Per specificare i siti delle reti sociali, sotto **Social Networks:** selezionare le caselle di controllo desiderate. Per ulteriori informazioni, consultare la descrizione del parametro Social Networks:.
- Per specificare i servizi e-mail basati sul Web, sotto **Web Mail Services:** selezionare le caselle di controllo desiderate. Per ulteriori informazioni, consultare la descrizione del parametro Web Mail Services:.

9. Fare clic su **OK**.

   La regola creata viene visualizzata sotto Rules nel riquadro destro della finestra di dialogo Protocols White List (Offline).

10. Fare clic su **OK** o su **Apply**.

    Gli utenti o i gruppi cui si applica una regola della lista bianca vengono visualizzati sotto White List nella struttura della console.

    Se nella struttura della console viene selezionato un utente o un gruppo cui si applica una regola della lista bianca, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:

    - **Protocol** - Il protocollo cui si applica la regola.
    - **Description** - Il nome della regola.
    - **Hosts** - Mostra gli host autorizzati per questa regola.

- **Ports** - Mostra le porte autorizzate per questa regola.
- **SSL** - Mostra l'opzione SSL selezionata. Valori possibili: **Allowed** (autorizza le connessioni SSL), **Denied** (nega le connessioni SSL) e **Required** (richiede l'utilizzo di SSL da parte di tutte le connessioni).
- **Extra parameters** - Mostra i parametri extra specifici per protocollo specificati per la regola. I parametri extra sono i seguenti: **From** (mostra gli ID dei mittenti autorizzati per la messaggistica immediata e gli indirizzi e-mail dei mittenti autorizzati per la Webmail) e **To** (mostra gli ID dei destinatari autorizzati per la messaggistica immediata e gli indirizzi dei destinatari autorizzati per la Webmail).
- **Profile** - Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

  È possibile definire più liste bianche dei protocolli online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire la lista bianca dei protocolli online, consultare la sezione "Gestione della lista bianca dei protocolli".

Modifica della lista bianca dei protocolli offline

È possibile modificare i valori dei parametri specificati per una regola della lista bianca offline in qualsiasi momento.

Per modificare una regola della lista bianca offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **White List**, scegliere **Manage Offline**, quindi attenersi alla procedura seguente:

   a) Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

   b) Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.

   - OPPURE -

Fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Edit**.

- OPPURE -

Sotto **Protocols**, espandere **White List**, quindi attenersi alla procedura seguente:

a) Sotto **White List**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi nel riquadro dei dettagli.
b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.
- OPPURE -
Nel riquadro dei dettagli, fare doppio clic sulla regola che si desidera modificare.

Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare i parametri della regola secondo le proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole della lista bianca dei protocolli offline

Per riutilizzare le regole esistenti della lista bianca dei protocolli offline, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Per copiare una regola della lista bianca offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Protocols White List (Offline).

4. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole della lista bianca applicate agli utenti o ai gruppi sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

5. Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. Se si usa la combinazione di tasti CTRL+X, la regola viene eliminata solo dopo essere stata incollata.

6. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro sinistro della finestra di dialogo Protocols White List (Offline).

8. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare gli utenti o i gruppi cui applicare la regola copiata.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/sui gruppi.

9. Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, fare clic con il pulsante destro del mouse nel riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro destro della finestra di dialogo Protocols White List (Offline).

10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione della lista bianca dei protocolli offline

È possibile esportare tutte le regole correnti della lista bianca dei protocolli offline in un file .pwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Per esportare la lista bianca dei protocolli offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Save Offline**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save Offline**.
     - OPPURE -
   - Espandere **White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola della lista bianca, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **White List**, selezionare qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage Offline**. Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .pwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   La lista bianca dei protocolli offline esportata viene salvata in un file con estensione .pwl.

Per importare la lista bianca dei protocolli offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.

b) Nella struttura della console, espandere **DeviceLock Service**.

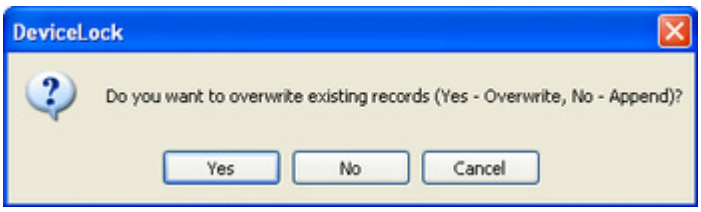
Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Load Offline**.
     - OPPURE -
   - Selezionare **White List**, quindi fare clic su **Load Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **White List**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load Offline**.
     - OPPURE -
   - Espandere **White List** e selezionare qualsiasi utente o gruppo specificato nella lista bianca. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola della lista bianca, quindi scegliere **Load**.
     - OPPURE -
   - Espandere **White List**, selezionare qualsiasi utente o gruppo specificato nella lista bianca, quindi scegliere **Load Offline** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage Offline**. Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, fare clic su **Load**.

   Viene visualizzata la finestra di dialogo Open.
4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   Se la lista bianca dei protocolli offline è già definita e si sceglie di importarne una nuova, viene visualizzato il seguente messaggio.



Nella finestra di messaggio, fare clic su **Yes** per sovrascrivere la lista bianca offline esistente. Fare clic su **No** per aggiungere la nuova lista bianca a quella esistente.

Eliminazione delle regole della lista bianca dei protocolli offline

Se alcune regole della lista bianca offline non sono più necessarie, possono essere eliminate.

Per eliminare una regola della lista bianca offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Espandere **White List**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo cui viene applicata la regola, quindi scegliere **Delete user**.
     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.
     - OPPURE -
   - Espandere **White List** e selezionare l'utente o il gruppo cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Manage Offline**. Nel riquadro sinistro della finestra di dialogo **Protocols White List (Offline)**, sotto **Users**, selezionare l'utente o il gruppo cui viene applicata la regola. Nel riquadro destro della finestra di dialogo **Protocols White List (Offline)**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.

Rimozione della definizione della lista bianca dei protocolli offline

È possibile riportare la lista bianca offline precedentemente definita allo stato non configurato. Se la lista bianca offline non è definita, ai computer client offline viene applicata la lista bianca Regular (normale).

Per rimuovere la definizione della lista bianca dei protocolli offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Undefine Offline**.

   Lo stato offline della lista bianca cambia in "Not Configured" (Non configurato).

   Selezionando **White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Protocols White List is not configured" (La lista bianca dei protocolli offline non è configurata).

Rimozione della lista bianca dei protocolli offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità della lista bianca offline di livello superiore e applicare la lista bianca normale a specifici gruppi di computer client di livello inferiore. Per applicare la lista bianca dei protocolli normale, occorre rimuovere le lista bianca dei protocolli offline.

Per rimuovere la lista bianca dei protocolli offline

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **White List**, quindi scegliere **Remove Offline**.

   Lo stato offline della lista bianca cambia in "Use Regular" (Usa normale).

   Selezionando **White List** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Protocols White List is configured to use Regular Protocols White List" (La lista bianca dei protocolli offline è configurata per l'utilizzo della lista bianca dei protocolli normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle regole basate sul contenuto offline per i protocolli

Per una descrizione dettagliata della funzione Content-Aware Rules (Regole basate sul contenuto) per i protocolli, consultare la sezione "Regole basate sul contenuto per i protocolli (Regular Profile)".

Le regole basate sul contenuto possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le regole basate sul contenuto non sono definite. Viene visualizzato il messaggio "Offline Content-Aware Rules are not configured" (Le regole basate sul contenuto offline non sono configurate). Si tratta dello stato predefinito.
Configured	Indica che le regole basate sul contenuto sono definite.
Use Regular	Indica che l'eredità delle regole basate sul contenuto offline è bloccata e sono applicate le regole basate sul contenuto Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle regole basate sul contenuto normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle regole basate sul contenuto normali consente di evitare che le regole basate sul contenuto offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle regole basate sul contenuto normali, consultare la sezione "Rimozione delle regole basate sul contenuto offline".

La gestione delle regole basate sul contenuto offline include le seguenti attività:

- Definizione delle regole basate sul contenuto offline
- Modifica delle regole basate sul contenuto offline
- Copia delle regole basate sul contenuto offline
- Esportazione e importazione delle regole basate sul contenuto offline
- Eliminazione delle regole basate sul contenuto offline
- Rimozione della definizione delle regole basate sul contenuto offline
- Rimozione delle regole basate sul contenuto offline

Definizione delle regole basate sul contenuto offline

Le regole basate sul contenuto (Content-Aware Rules) vengono create in base ai gruppi di contenuto incorporati o personalizzati. Per informazioni dettagliate su questi gruppi, consultare la sezione "Configurazione delle impostazioni di rilevamento del contenuto".

Per definire una regola basata sul contenuto (Content-Aware Rule) offline

1. Se si utilizza DeviceLock Management Console:

a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

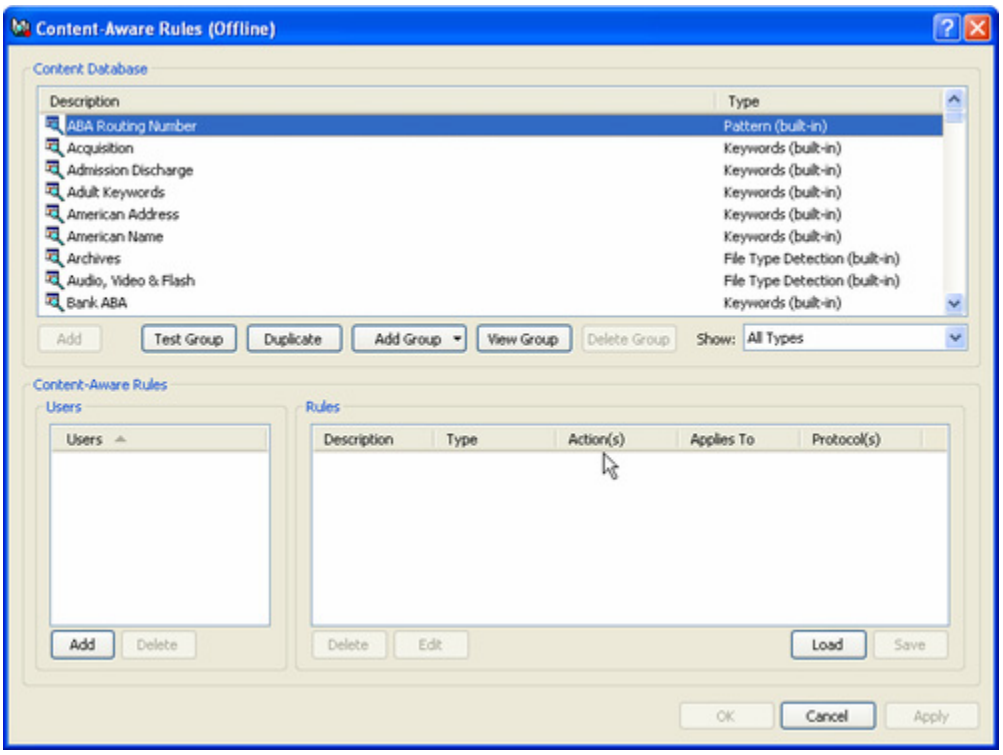
a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules (Offline).



4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

5. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o gruppi per cui si desidera definire la regola, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules (Offline).

   Per eliminare un utente o un gruppo, nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo desiderato, quindi fare clic su **Delete** o premere il tasto CANC.

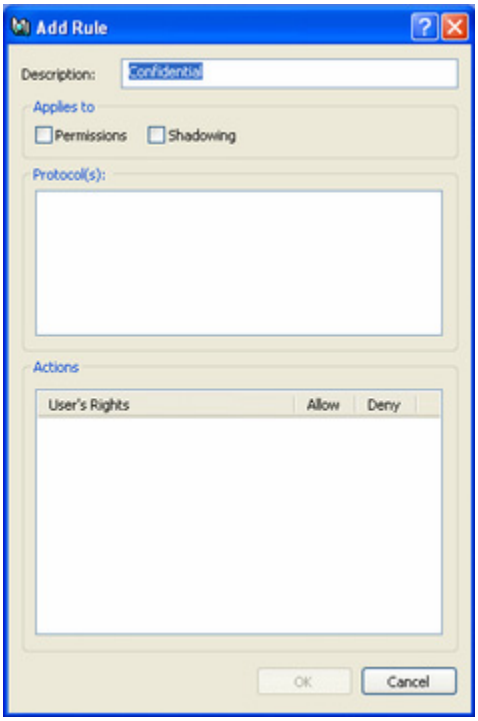
6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare gli utenti o i gruppi per cui si desidera definire la regola.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

7. Nel riquadro superiore della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Content Database**, selezionare il gruppo di contenuto desiderato e fare clic su **Add**.

   Nota: è possibile specificare un solo gruppo di contenuto per ogni regola basata sul contenuto.

   Viene visualizzata la finestra di dialogo Add Rule.



8. Nella finestra di dialogo **Add Rule**, nella casella **Description**, digitare il nome della regola basata sul contenuto.

   Per impostazione predefinita, quest'ultima ha lo stesso nome del gruppo di contenuto specificato, ma è possibile specificare un altro nome.

9. Sotto **Applies to**, specificare il tipo di operazione associata alla regola. Le opzioni disponibili sono:
   - **Permissions**: specifica che la regola verrà applicata alle operazioni di controllo dell'accesso.
   - **Shadowing**: specifica che la regola verrà applicata alle operazioni di copia shadow.
   - **Permissions, Shadowing**: specifica che la regola verrà applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.
10. Sotto **Protocol(s)**, selezionare i protocolli appropriati a cui si desidera applicare la regola.

    Le regole basate sul contenuto possono essere applicate ai seguenti protocolli: FTP, HTTP, ICQ/AOL Messenger, IRC, Jabber, Mail.ru Agent, SMTP, Social Networks, Web Mail, Windows Messenger e Yahoo Messenger.

    Se vengono selezionati più protocolli con diversi diritti di accesso, nella finestra di dialogo sotto Action(s) vengono visualizzati solo i diritti di accesso comuni per tutti i protocolli selezionati.
11. Sotto **Action(s)**, specificare quali azioni degli utenti sono autorizzate o non autorizzate per i protocolli e quali azioni degli utenti vanno inserite in Shadow Log.

    Per informazioni dettagliate sui diritti degli utenti che possono essere specificati nelle regole basate sul contenuto (Content-Aware Rules), consultare le sezioni "Regole basate sul contenuto per le operazioni di controllo dell'accesso" e "Regole basate sul contenuto per le operazioni di copia shadow".
12. Fare clic su **OK**.

    La regola creata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules (Offline).
13. Fare clic su **OK** o su **Apply** per applicare la regola.

    Gli utenti o i gruppi per cui è stata applicata la regola basata sul contenuto vengono visualizzati sotto Content-Aware Rules nella struttura della console. Se nella struttura della console viene selezionato un utente o un gruppo per cui è stata applicata una regola basata sul contenuto, nel riquadro dei dettagli vengono visualizzate informazioni dettagliate sulla regola. Le informazioni includono:
    - **Description**: il nome della regola. Per impostazione predefinita, la regola ha lo stesso nome del gruppo di contenuto specificato.
    - **Type**: il tipo di analisi del contenuto. Valori possibili: **File Type Detection**, **Keywords**, **Pattern**, **Document Properties** e **Complex**. **File Type Detection** indica che il riconoscimento e l'identificazione dei file si basa sulle loro firme caratteristiche. **Keywords** indica che il riconoscimento e l'identificazione dei file/dati si basa sulle parole chiave o frasi specificate. **Pattern** indica che il riconoscimento e l'identificazione dei file/dati si basa sui motivi di testo specificati descritti dalle espressioni comuni Perl. **Document Properties** indica che il riconoscimento e l'identificazione dei file si basa sulle loro proprietà. **Complex** indica che il riconoscimento e l'identificazione dei file/dati si basa sul contenuto specificato descritto da un'espressione booleana.

- **Action(s)**: mostra quali azioni degli utenti sono autorizzate o non autorizzate per i protocolli e quali azioni degli utenti vanno inserite in Shadow Log.
- **Applies To**: Valori possibili: **Permissions**, **Shadowing** e **Permissions, Shadowing**. **Permissions** indica che la regola viene applicata alle operazioni di controllo dell'accesso. **Shadowing** indica che la regola viene applicata alle operazioni di copia shadow. **Permissions, Shadowing** indica che la regola viene applicata sia alle operazioni di controllo dell'accesso sia a quelle di copia shadow.
- **Protocol(s)**: i protocolli per cui viene applicata la regola.
- **Profile**: Valori possibili: **Regular** e **Offline**. **Regular** indica che la regola viene applicata ai computer client che operano online. **Offline** indica che la regola viene applicata ai computer che operano offline.

  È possibile definire diverse regole basate sul contenuto online od offline per lo stesso utente o gli stessi gruppi di utenti. Per informazioni su come definire le regole basate sul contenuto online per i protocolli, consultare la sezione "Gestione delle regole basate sul contenuto".

Modifica delle regole basate sul contenuto offline

È possibile modificare le proprietà delle regole basate sul contenuto (Content-Aware Rule) come Description, Applies To, Protocol(s) e Actions.

Come modificare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, scegliere **Manage Offline**, quindi attenersi alla procedura seguente:
   a) Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.

      Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.
   b) Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, selezionare la regola da modificare, quindi fare clic su **Edit**.

   - OPPURE -

Sotto **Protocols**, espandere **Content-Aware Rules**, quindi attenersi alla procedura seguente:

a) Sotto **Content-Aware Rules**, selezionare l'utente o il gruppo per cui si desidera modificare la regola.
Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto applicati agli stessi nel riquadro dei dettagli.

b) Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola che si desidera eliminare e selezionare **Edit**.
- OPPURE -
Nel riquadro dei dettagli, fare doppio clic sulla regola che si desidera modificare.

Viene visualizzata la finestra di dialogo Edit Rule.

4. Nella finestra di dialogo **Edit Rule**, modificare le proprietà della regola a seconda delle proprie esigenze.
5. Fare clic su **OK** o per applicare le modifiche.

Copia delle regole basate sul contenuto offline

Per riutilizzare le regole basate sul contenuto (Content-Aware Rules) offline esistenti, è possibile eseguire un'operazione taglia/incolla, copia/incolla o di trascinamento.

Come copiare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Manage Offline** sulla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Content-Aware Rules (Offline).

4. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola da copiare.

   Selezionando gli utenti o i gruppi, è possibile visualizzare le regole basate sul contenuto sotto Rules, nel riquadro inferiore destro della finestra di dialogo.

5. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic con il pulsante destro del mouse sulla regola da copiare, quindi scegliere **Copy** o **Cut**.

   La regola copiata (Copy) o tagliata (Cut) viene copiata automaticamente negli Appunti.

   È possibile utilizzare le combinazioni di tasti CTRL+C, CTRL+X e CTRL+V per copiare, tagliare e incollare la regola. Se si usa la combinazione di tasti CTRL+X, la regola viene tagliata solo dopo essere stata incollata.

   Per eseguire un'operazione di trascinamento, selezionare la regola e spostarla verso l'utente o il gruppo a cui si desidera applicare la regola copiata.

6. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, fare clic su **Add**.

   Viene visualizzata la finestra di dialogo Select Users or Groups.

7. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare i nomi degli utenti o dei gruppi a cui si desidera applicare la regola copiata, quindi fare clic su **OK**.

   Gli utenti e i gruppi aggiunti vengono visualizzati sotto Users nel riquadro inferiore sinistro della finestra di dialogo Content-Aware Rules (Offline).

8. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare gli utenti o i gruppi a cui applicare la regola copiata.

   È possibile selezionare più utenti o gruppi tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sugli utenti/gruppi.

9. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, fare clic con il pulsante destro del mouse sul riquadro **Rules**, quindi scegliere **Paste**.

   La regola copiata viene visualizzata sotto Rules nel riquadro inferiore destro della finestra di dialogo Content-Aware Rules (Offline).

10. Fare clic su **OK** o su **Apply** per applicare la regola copiata.

Esportazione e importazione delle regole basate sul contenuto offline

È possibile esportare tutte le Content-Aware Rules (regole basate sul contenuto) offline correnti in un file .cwl che, a sua volta, può essere importato e utilizzato su un altro computer. Le operazioni di esportazione e l'importazione delle regole possono essere utilizzate anche a fini di backup.

Come esportare le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Save Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo, quindi scegliere **Save Offline**.
     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Save**.
     - OPPURE -
   - Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Save Offline** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic su **Save**.

   Viene visualizzata la finestra di dialogo di salvataggio Save As.

4. Nella finestra di dialogo **Save As**, nella casella **Save in**, selezionare la posizione in cui salvare il file .cwl.
5. Nella casella **File name**, digitare il nome di file desiderato.
6. Fare clic su **Save**.

   Le regole esportate vengono salvate in un file con estensione .cwl.

Come importare le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:

   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Load Offline**.
     - OPPURE -
   - Selezionare **Content-Aware Rules**, quindi fare clic su **Load Offline** sulla barra degli strumenti.
     - OPPURE -
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse su qualsiasi utente o gruppo, quindi scegliere **Load Offline**.
     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare qualsiasi utente o gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola, quindi scegliere **Load**.
     - OPPURE -
   - Espandere **Content-Aware Rules**, selezionare qualsiasi utente o gruppo a cui viene applicata la regola, quindi fare clic su **Load Offline** sulla barra degli strumenti.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, fare clic su **Load**.

   Viene visualizzata la finestra di dialogo Open.

4. Nella finestra di dialogo **Open**, nell'elenco **Look in**, fare clic sulla posizione che contiene il file da importare.
5. Nell'elenco delle cartelle, individuare e aprire la cartella che contiene il file.
6. Fare clic sul file, quindi scegliere **Open**.

   È possibile importare un solo file .cwl alla volta.

Eliminazione delle regole basate sul contenuto offline

Quando alcune Content-Aware Rules (regole basate sul contenuto) offline non sono più necessarie, possono essere eliminate.

Come eliminare una regola basata sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
   a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:
   - Espandere **Content-Aware Rules**, fare clic con il pulsante destro del mouse sull'utente o sul gruppo a cui viene applicata la regola, quindi scegliere **Delete user**.
     Quando viene eliminato un utente o un gruppo, la regola associata con l'utente o il gruppo viene automaticamente eliminata.

     - OPPURE -
   - Espandere **Content-Aware Rules** e selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sulla regola associata con questo utente o gruppo, quindi scegliere **Delete**.
     - OPPURE -
   - Fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Manage Offline**. Nel riquadro inferiore sinistro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Users**, selezionare l'utente o il gruppo a cui viene applicata la regola. Nel riquadro inferiore destro della finestra di dialogo **Content-Aware Rules (Offline)**, sotto **Rules**, selezionare la regola da modificare e fare clic su **Delete**, oppure fare clic con il pulsante destro del mouse sulla regola e scegliere **Delete**.
     È possibile selezionare più regole da eliminare tenendo premuto il tasto MAIUSC o CTRL mentre si fa clic sulle regole.

Rimozione della definizione delle regole basate sul contenuto offline

È possibile riportare le regole basate sul contenuto offline precedentemente definite al loro stato non configurato. Se le regole offline non sono definite, ai computer client offline vengono applicate le regole normali.

Come rimuovere la definizione delle regole basate sul contenuto offline

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.
    b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Service Settings Editor:
    a) Aprire DeviceLock Service Settings Editor.
    b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
    a) Aprire Group Policy Object Editor.
    b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Undefine Offline**.

   Lo stato offline delle regole basate sul contenuto cambia in "Not Configured" (Non configurato).

   Selezionando **Content-Aware Rules** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Content-Aware Rules are not configured" (Le regole basate sul contenuto offline non sono configurate).

Rimozione delle regole basate sul contenuto offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle regole basate sul contenuto offline di livello superiore e applicare le regole basate sul contenuto normali a specifici gruppi di computer client di livello inferiore. Per applicare le regole basate sul contenuto Regular (normali), occorre rimuovere le regole basate sul contenuto offline.

Come rimuovere le regole basate sul contenuto offline

1. Se si utilizza DeviceLock Service Settings Editor:
    a) Aprire DeviceLock Service Settings Editor.
    b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:
    a) Aprire Group Policy Object Editor.
    b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.
2. Espandere **Protocols**.
3. Sotto **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules**, quindi scegliere **Remove Offline**.

   Lo stato offline delle regole basate sul contenuto cambia in "Use Regular" (Usa normale).

Selezionando **Content-Aware Rules** nella struttura della console, nel riquadro dei dettagli viene visualizzato il seguente messaggio: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules" (Le regole basate sul contenuto offline sono configurate per l'utilizzo delle regole basate sul contenuto normali).

Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Gestione delle impostazioni di protezione offline per i protocolli

Per una descrizione dettagliata della funzione Security Settings (Impostazioni di protezione) per i protocolli, consultare la sezione "Gestione delle impostazioni di protezione per i protocolli".

Le impostazioni di protezione offline possono presentare uno dei seguenti stati:

STATO	DESCRIZIONE
Not Configured	Indica che le impostazioni di protezione non sono definite per i protocolli. Si tratta dello stato predefinito.
Enabled	Indica che le impostazioni di protezione sono definite per i protocolli.
Disabled	Indica che le impostazioni di protezione sono disattivate per i protocolli.
Use Regular	Indica che l'eredità delle impostazioni di protezione offline è bloccata e sono applicate le impostazioni di protezione Regular (normali). Le impostazioni offline di DeviceLock possono disporre di questo stato solo in DeviceLock Service Settings Editor o DeviceLock Group Policy Manager. L'applicazione delle impostazioni di protezione normali è consigliabile se si utilizzano Group Policy o i file DeviceLock Service Settings (.dls) per applicare i criteri di DeviceLock all'interno della rete. L'applicazione delle impostazioni di protezione normali consente di evitare che le impostazioni di protezione offline ereditate da un livello superiore vengano applicate a un gruppo specifico di computer client di livello inferiore. Per maggiori informazioni sull'applicazione delle impostazioni di protezione normali, consultare la sezione "Rimozione delle impostazioni di protezione offline".

La gestione delle impostazioni di protezione offline prevede le seguenti attività:

- Definizione e modifica delle impostazioni di protezione offline
- Rimozione della definizione delle impostazioni di protezione offline
- Rimozione delle impostazioni di protezione offline

Definizione e modifica delle impostazioni di protezione offline

Per definire e modificare le impostazioni di protezione offline

1. Se si utilizza DeviceLock Management Console:
    a) Aprire DeviceLock Management Console e collegarla al computer in cui è in esecuzione DeviceLock Service.

b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

- Selezionare **Security Settings**. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sull'impostazione di protezione, quindi scegliere **Enable Offline** o **Disable Offline**.
  Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

  - OPPURE-

- Fare clic con il pulsante destro del mouse su **Security Settings**, quindi scegliere **Manage Offline**. Nella finestra di dialogo **Security Settings (Offline)** visualizzata, selezionare o deselezionare le caselle di controllo pertinenti e fare clic su **OK**.
  La finestra di dialogo Security Settings (Offline) può essere inoltre aperta selezionando Security Settings e, in seguito, facendo clic su Manage Offline *sulla barra degli strumenti.*

Nota: tutte le caselle di controllo della finestra di dialogo **Security Settings (Offline)** presentano tre stati: selezionato, deselezionato e indeterminato, corrispondenti agli stati Enabled (Abilitato), Disabled (Disabilitato) e Not Configured (Non configurato) delle impostazioni di protezione.

Lo stato offline dell'impostazione di protezione cambia da "Not Configured" (Non configurato) a "Enabled" (Abilitato) o "Disabled" (Disabilitato).

Rimozione della definizione delle impostazioni di protezione offline

È possibile riportare le impostazioni di protezione precedentemente definite allo stato non configurato. Se le impostazioni di protezione offline non sono definite, ai computer client offline vengono applicate le impostazioni di protezione normali.

Per rimuovere la definizione delle impostazioni di protezione offline

1. Se si utilizza DeviceLock Service Settings Editor:

a) Aprire DeviceLock Service Settings Editor.
b) Nella struttura della console, fare clic con il pulsante destro del mouse su **DeviceLock Settings** o **DeviceLock Service**, quindi selezionare **Load Service Settings** per aprire il file XML contenente i criteri di DeviceLock definiti.
c) Nella struttura della console, espandere **DeviceLock Service**.

Se si utilizza DeviceLock Group Policy Manager:

a) Aprire Group Policy Object Editor.
b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, eseguire una delle seguenti azioni:

- Selezionare **Security Settings**. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse sull'impostazione di protezione, quindi scegliere **Undefine Offline**.

  Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

  - OPPURE-

- Fare clic con il pulsante destro del mouse su **Security Settings**, quindi scegliere **Manage Offline**. Nella finestra di dialogo **Security Settings (Offline)** visualizzata, impostare nuovamente le caselle di controllo appropriate sullo stato indeterminato e fare clic su **OK**.

  La finestra di dialogo Security Settings (Offline) può essere inoltre aperta selezionando Security Settings e, in seguito, facendo clic su Manage Offline *sulla barra degli strumenti.*

Nota: tutte le caselle di controllo della finestra di dialogo **Security Settings (Offline)** presentano tre stati: selezionato, deselezionato e indeterminato, corrispondenti agli stati Enabled (Abilitato), Disabled (Disabilitato) e Not Configured (Non configurato) delle impostazioni di protezione.

Lo stato offline dell'impostazione di protezione cambia in "Not Configured" (Non configurato).

Rimozione delle impostazioni di protezione offline

Se i criteri di DeviceLock vengono implementati tramite Group Policy o file DeviceLock Service Settings (.dls), DeviceLock consente di bloccare l'eredità delle impostazioni di protezione offline di livello superiore e applicare le impostazioni di protezione normali a specifici gruppi di computer client di livello inferiore. Per applicare le impostazioni di protezione normali, occorre rimuovere le impostazioni di protezione offline.

Come rimuovere le impostazioni di protezione offline

1. Se si utilizza DeviceLock Service Settings Editor:

   a) Aprire DeviceLock Service Settings Editor.
   b) Nella struttura della console, espandere **DeviceLock Service**.

   Se si utilizza DeviceLock Group Policy Manager:

   a) Aprire Group Policy Object Editor.
   b) Nella struttura della console, espandere **Computer Configuration**, quindi **DeviceLock**.

2. Espandere **Protocols**.
3. Sotto **Protocols**, selezionare **Security Settings**.

   Dopo aver selezionato Security Settings nella struttura della console, le opzioni vengono visualizzate nel riquadro dei dettagli.

4. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su qualsiasi impostazione di protezione da rimuovere, quindi scegliere **Remove Offline**.

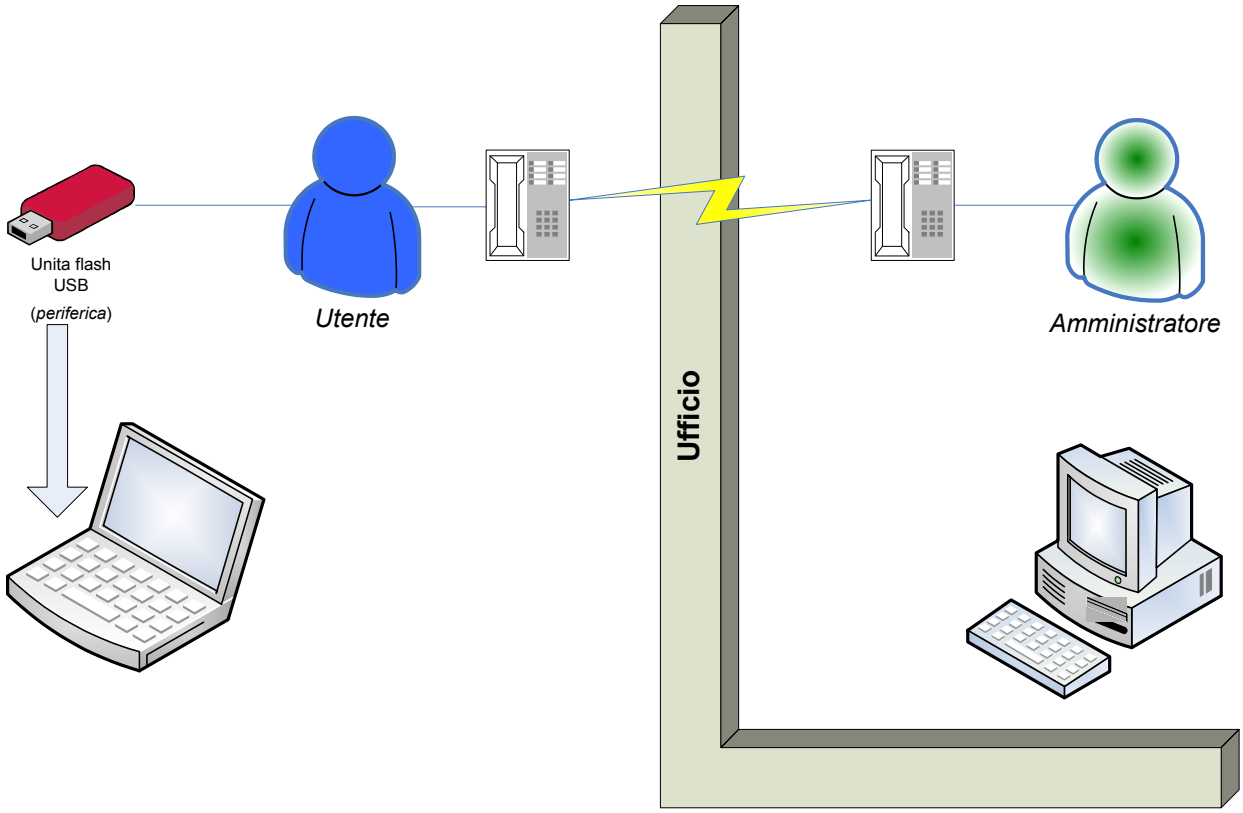
   Lo stato offline delle impostazioni di protezione cambia in "Use Regular" (Usa normale).

   Lo stato "Use Regular" delle impostazioni di DeviceLock viene visualizzato come "Not Configured" (Non configurato) su DeviceLock Management Console.

Temporary White List

Introduzione

La funzione Temporary White List di DeviceLock consente l'accesso temporaneo alle periferiche USB quando non si dispone di una connessione di rete. Gli amministratori forniscono telefonicamente agli utenti dei codici speciali che concedono temporaneamente l'accesso alle periferiche richieste.



Il principio di funzionamento di una white list temporanea è simile a quello di una white list delle periferiche, con la differenza che per aggiungere una periferica ad una white list temporanea e per concedere l'accesso a tale periferica, non è necessaria una connessione di rete.

Nota: l'utilizzo di una white list temporanea permette di concedere l'accesso alle periferiche USB bloccate sia a livello di porta USB sia a livello di tipo. Se una periferica elencata nella white list (ad esempio un'unità flash USB) appartiene a entrambi i livelli: USB e tipo (Removable), le eventuali autorizzazioni sia per il livello di tipo sia per il livello USB vengono ignorate.

Per creare e attivare una white list temporanea, eseguire i seguenti passaggi:

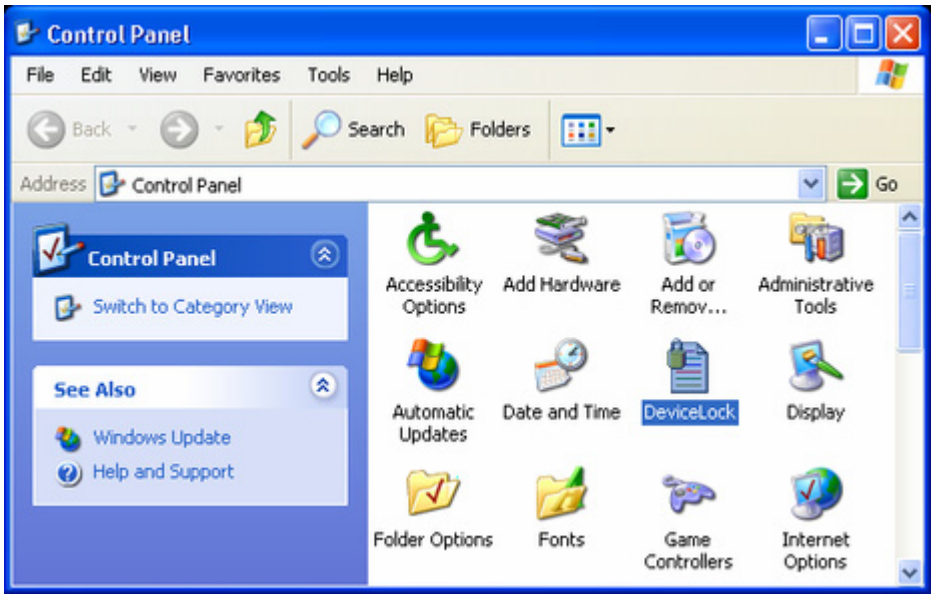
1. L'amministratore utilizza lo strumento Certificate Generation per creare un certificato crittografato (certificato di DeviceLock). Il certificato di DeviceLock è composto da una chiave pubblica e da una chiave privata.

2. L'amministratore distribuisce il certificato di DeviceLock (la chiave pubblica) all'utente del computer per consentirgli l'attivazione della white list temporanea sulla propria macchina.
3. Quando un utente deve accedere ad una periferica USB, esegue lo strumento Temporary White List Authorization dal Pannello di controllo di Windows, seleziona la periferica da un elenco e attende la generazione di un codice alfanumerico (**Device Code**). Una volta ottenuto questo codice, lo fornisce all'amministratore di DeviceLock telefonicamente o via Internet, in una sessione di chat.
4. L'amministratore esegue quindi lo strumento DeviceLock Signing Tool, carica il certificato DeviceLock Certificate corrispondente (la chiave privata), immette il codice (**Device Code**), seleziona un periodo di accesso temporaneo appropriato (5, 15 minuti, ecc., fino a quando la periferica non viene scollegata o fino a quando l'utente non si scollega), genera un codice di sblocco (**Unlock Code**) e lo fornisce all'utente.
5. Una volta ottenuto il codice di sblocco (**Unlock Code**), l'utente lo digita nell'applet Temporary White List Authorization. Ora, l'utente è autorizzato a utilizzare la periferica per il periodo di tempo specificato.

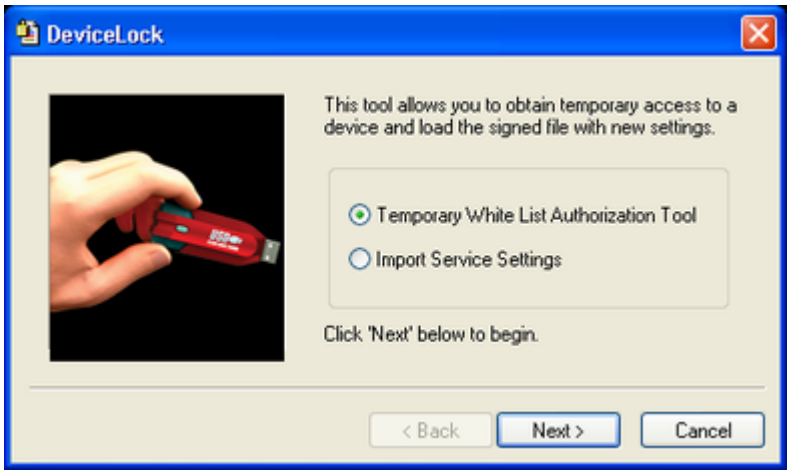
Strumento Temporary White List Authorization

Lo strumento Temporary White List Authorization è un'applet del Pannello di controllo che gli utenti devono utilizzare per richiedere l'accesso temporaneo alle periferiche.

Per avviare lo strumento di autorizzazione, l'utente deve eseguire l'applet **DeviceLock** dal Pannello di controllo e selezionare l'opzione **Temporary White List Authorization Tool**.

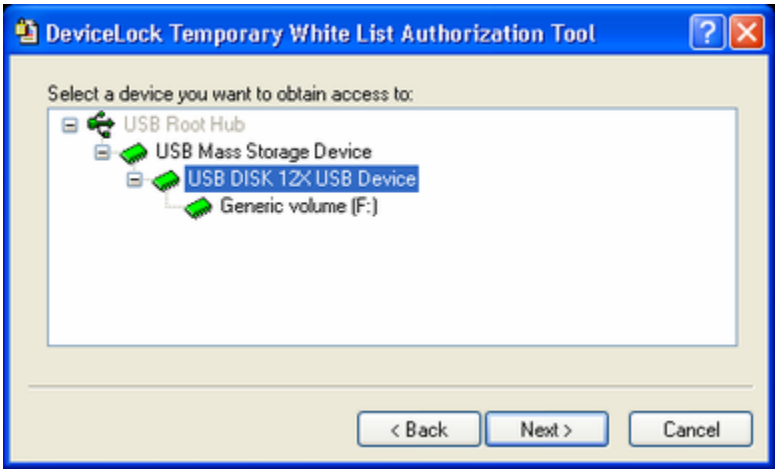


Nota: in Windows XP e versioni successive, per visualizzare tutte le applet del Pannello di controllo, è necessario visualizzare le icone del Pannello di controllo in modalità classica.

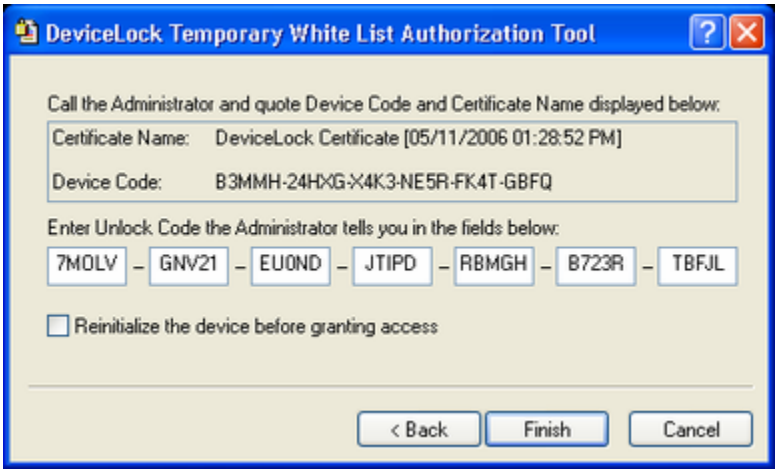

DeviceLock
This tool allows you to obtain temporary access to a device and load the signed file with new settings.
Temporary White List Authorization Tool
Import Service Settings
Click 'Next' below to begin.
< Back
Next >
Cancel

Per richiedere ed ottenere l'accesso temporaneo ad una periferica, l'utente deve eseguire cinque semplici passaggi:

1. Collegare la periferica a cui desidera accedere alla porta USB.
2. Selezionare la periferica dall'elenco delle periferiche USB disponibili.


DeviceLock Temporary White List Authorization Tool
Select a device you want to obtain access to:
USB Root Hub
USB Mass Storage Device
USB DISK 12X USB Device
Generic volume (F:)
< Back
Next >
Cancel

3. Contattare l'amministratore e comunicargli il nome del certificato ed il codice **Device Code**. Il codice **Device Code** ha validità di 24 ore, a partire dall'ora in cui è stato generato dall'applet.


DeviceLock Temporary White List Authorization Tool
Call the Administrator and quote Device Code and Certificate Name displayed below:
Certificate Name: DeviceLock Certificate [05/11/2006 01:28:52 PM]
Device Code: B3MMH-24HXG-X4K3-NE5R-FK4T-GBFQ
Enter Unlock Code the Administrator tells you in the fields below:
7MOLV - GNV21 - EU0ND - JTIPD - RBMGH - B723R - TBFJL
Reinitialize the device before granting access
< Back
Finish
Cancel

4. Immettere il codice di sblocco (**Unlock Code**) ricevuto dall'amministratore.

   Se è necessario forzare la reinizializzazione della periferica prima di potervi accedere, ovvero se è necessario scollegarla e ricollegarla alla porta, selezionare la casella di controllo **Reinitialize device before granting access**.

   Alcune periferiche USB, quali i mouse, non funzionano se non vengono reinizializzate. Pertanto, è preferibile selezionare sempre questa casella di controllo.

   Si consiglia di tenere deselezionata la casella di controllo **Reinitialize device before granting access** per le periferiche di archiviazione (quali le unità flash, CD/DVD-ROM, dischi fissi esterni e così via).

   Alcune periferiche USB non possono essere reinizializzate da DeviceLock Service. Ciò significa che i relativi driver non supportano la reinizializzazione via software. Se nella white list è presente una periferica di questo tipo e la periferica non funziona, per riavviare il driver della periferica è necessario che l'utente rimuova la periferica dalla porta e la inserisca manualmente nuovamente.

5. Infine, premere il pulsante **Finish**. Se il codice di sblocco (**Unlock Code**) immesso è valido, sarà possibile accedere alla periferica in pochi secondi.

Se è stata attivata la registrazione delle modifiche nelle impostazioni del servizio, tutti i tentativi riusciti di aggiungere le periferiche alla white list temporanea vengono registrati.

Appendice

Esempi di autorizzazioni e controllo per le periferiche

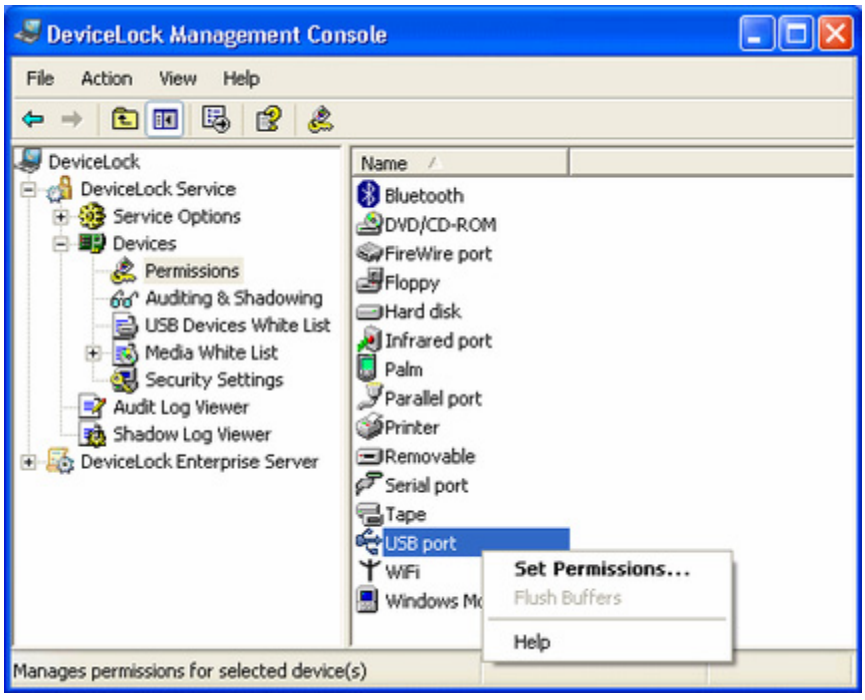
I seguenti esempi consentono di comprendere meglio come impostare in modo corretto le autorizzazioni e le regole di controllo e di shadowing in DeviceLock.

Per tutti gli esempi, si suppone che si stia utilizzando DeviceLock Management Console (lo snap-in MMC) e che questo sia già connesso al computer su cui è in esecuzione DeviceLock Service. Per ulteriori informazioni sull'utilizzo di DeviceLock Management Console, leggere la sezione DeviceLock Management Console.

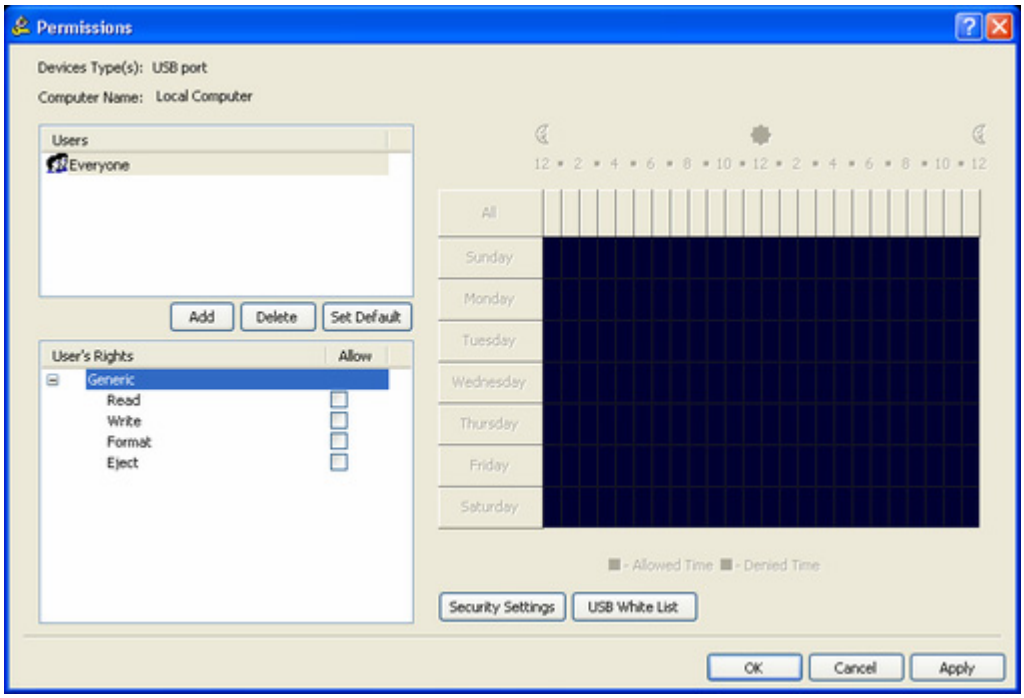
Esempi di autorizzazioni

Impedire a qualsiasi utente l'utilizzo delle periferiche USB ad eccezione della tastiera e del mouse:

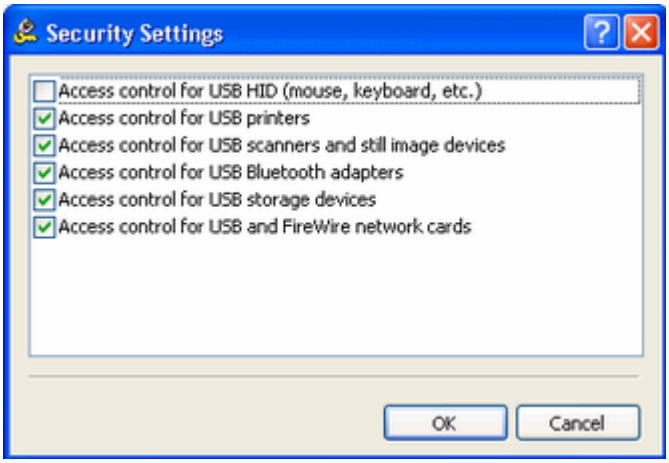
1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse su **USB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.



2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (digitarne il nome o cercare i nomi disponibili e selezionare quello desiderato), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e disattivare tutti i diritti nell'elenco **User's Rights**.



3. Fare clic sul pulsante **Security Settings** nella finestra di dialogo **Permissions** e quindi deselezionare la casella di controllo **Access control for USB HID (mouse, keyboard, etc.)**, come mostrato nella seguente immagine.

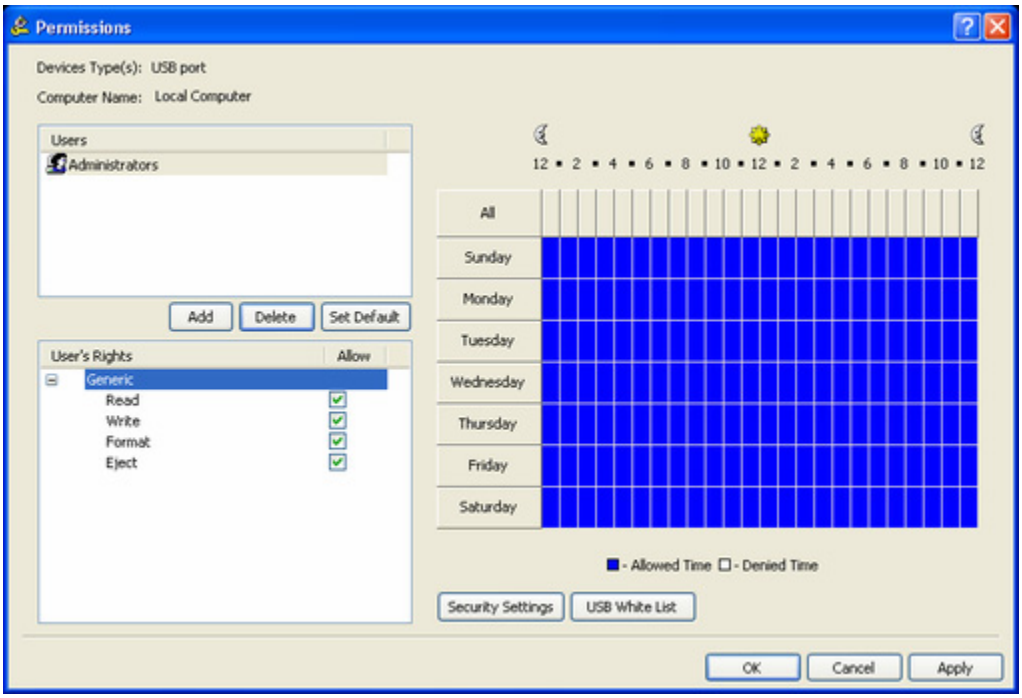

Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Fare clic sul pulsante **OK** per chiudere la finestra di dialogo **Security Settings**, scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**, quindi fare clic sul pulsante **Yes** per confermare la scelta.

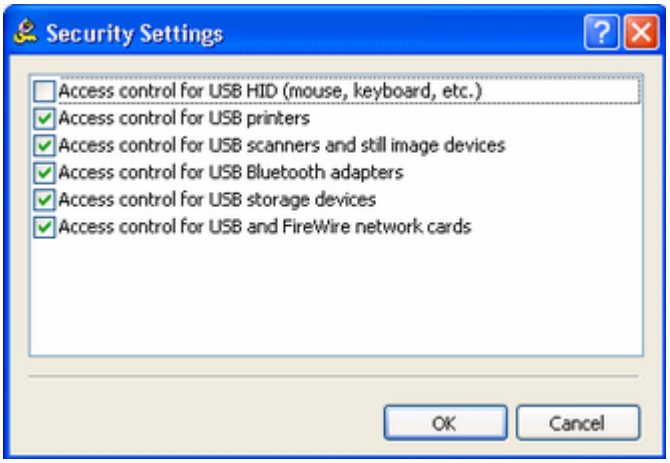
Impedire a qualsiasi utente l'utilizzo delle periferiche USB ad eccezione della tastiera e del mouse, ma consentire ai membri del gruppo Administrators l'utilizzo di tutte le periferiche USB:

1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse su **USB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.

2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere il gruppo **Administrators** (digitarne il nome o cercare i nomi disponibili e selezionare quello desiderato), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Administrators** e attivare tutti i diritti nell'elenco **User's Rights**.



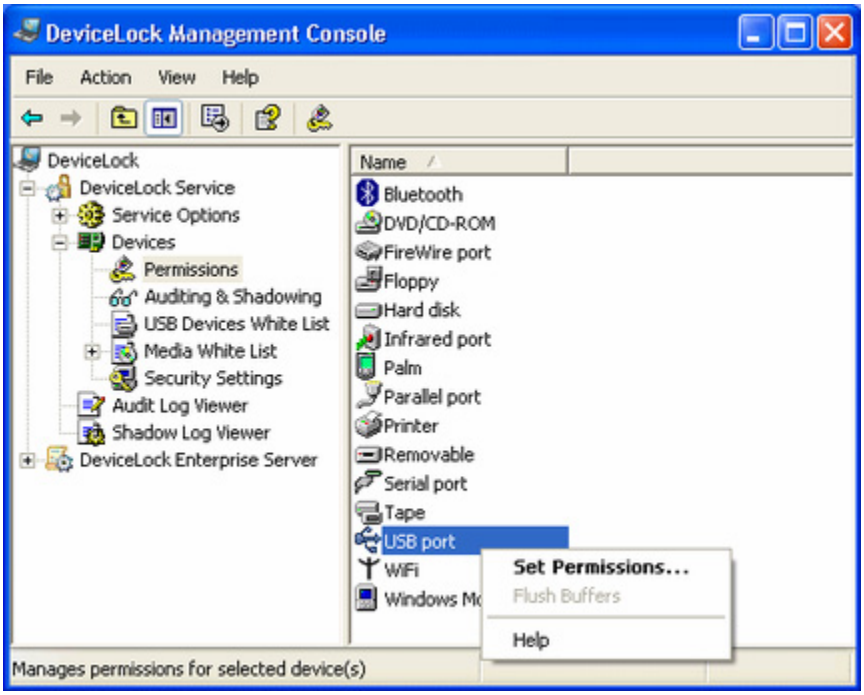
3. Fare clic sul pulsante **Security Settings** nella finestra di dialogo **Permissions** e quindi deselezionare la casella di controllo **Access control for USB HID (mouse, keyboard, etc.)**, come mostrato nella seguente immagine.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

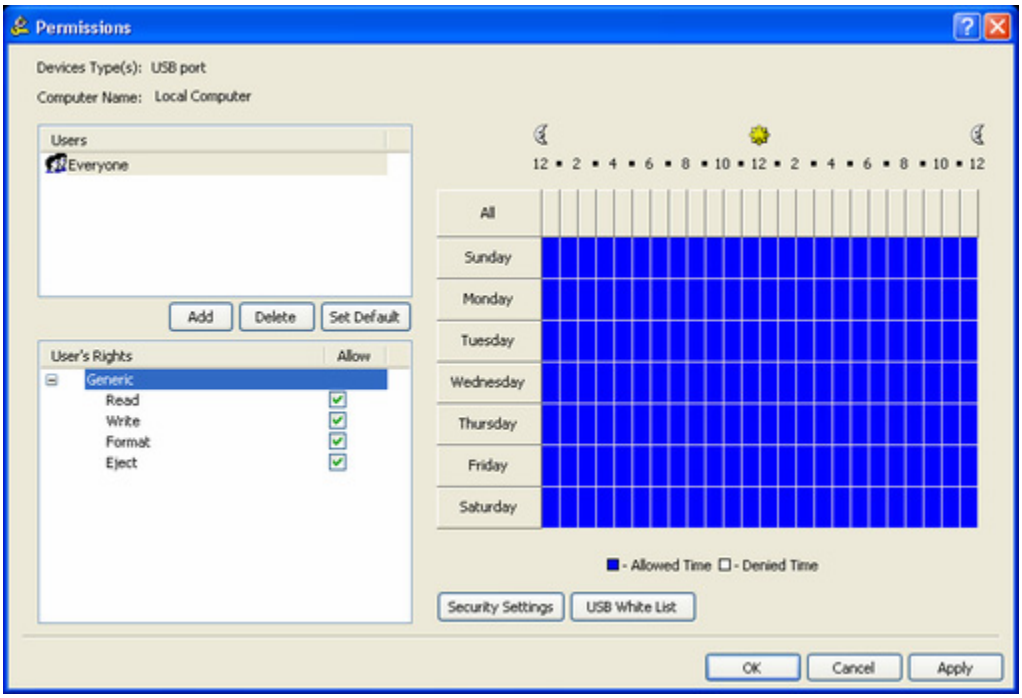
4. Fare clic sul pulsante **OK** per chiudere la finestra di dialogo **Security Settings** e quindi scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**.

Impedire a qualsiasi utente l'accesso alle periferiche di archiviazione, ad eccezione dei dischi fissi, e consentire l'accesso alle periferiche USB non di archiviazione:

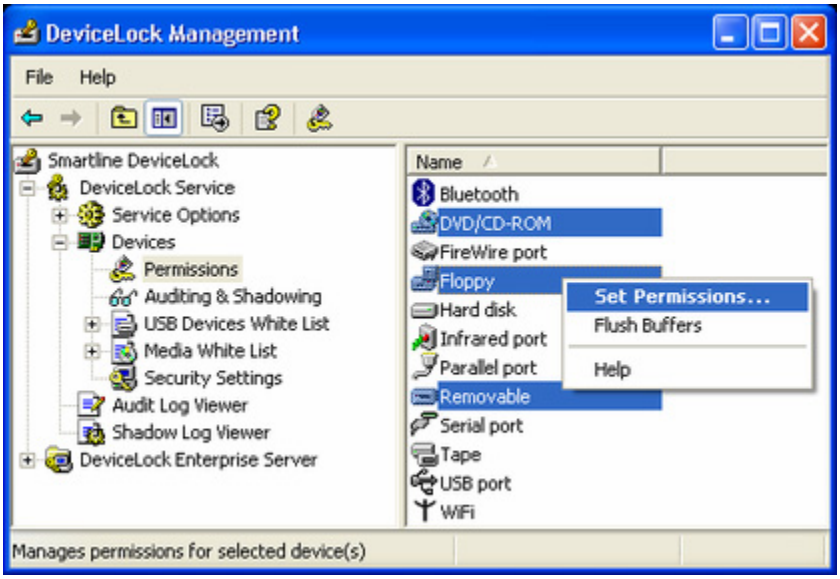
1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse su **USB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.



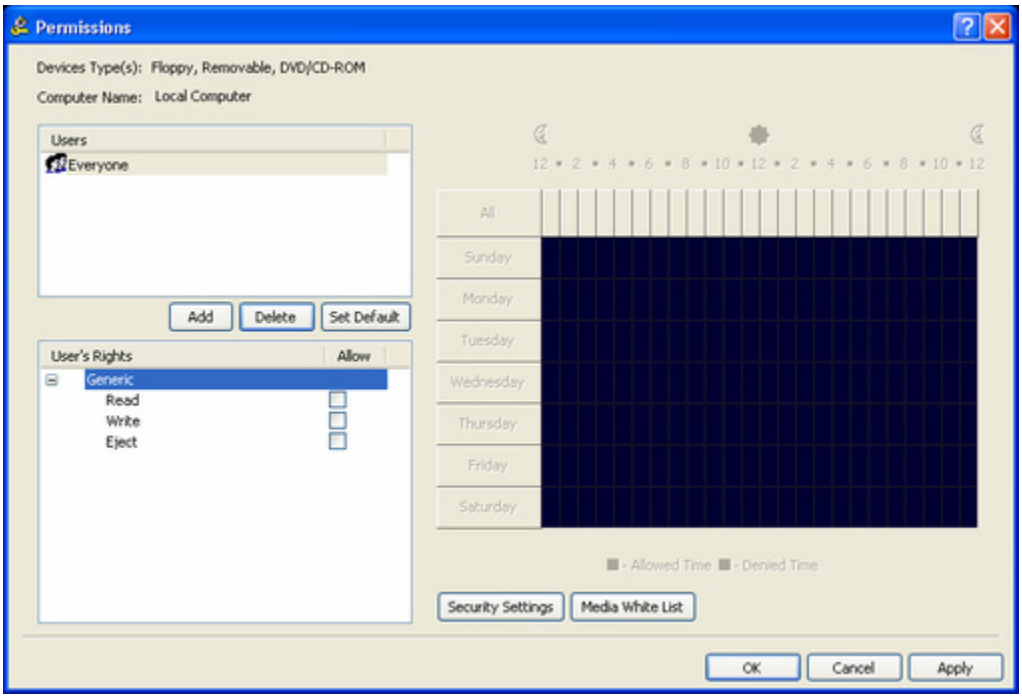
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (digitarne il nome o cercare i nomi disponibili e selezionare quello desiderato), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e attivare tutti i diritti nell'elenco **User's Rights**.



3. Scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**.
4. Selezionare la sezione **Permissions**, evidenziare le voci **DVD/CD-ROM**, **Floppy** e **Removable** nell'elenco dei tipi di periferica, fare clic con il pulsante destro del mouse e quindi scegliere **Set Permissions** dal menu sensibile al contesto.



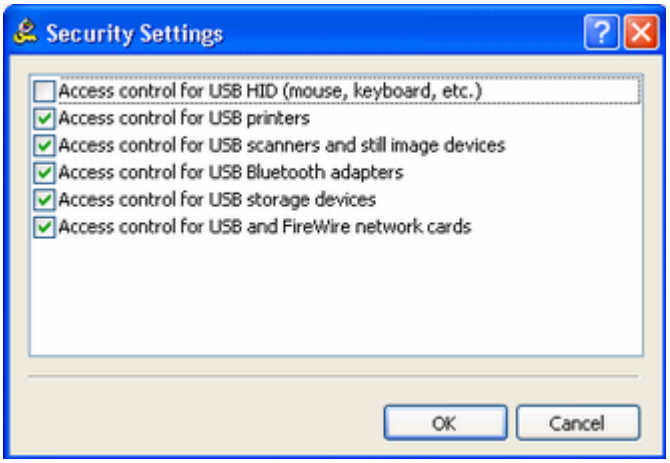
5. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (digitarne il nome o cercare i nomi disponibili e selezionare quello desiderato), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e disattivare tutti i diritti nell'elenco **User's Rights**.



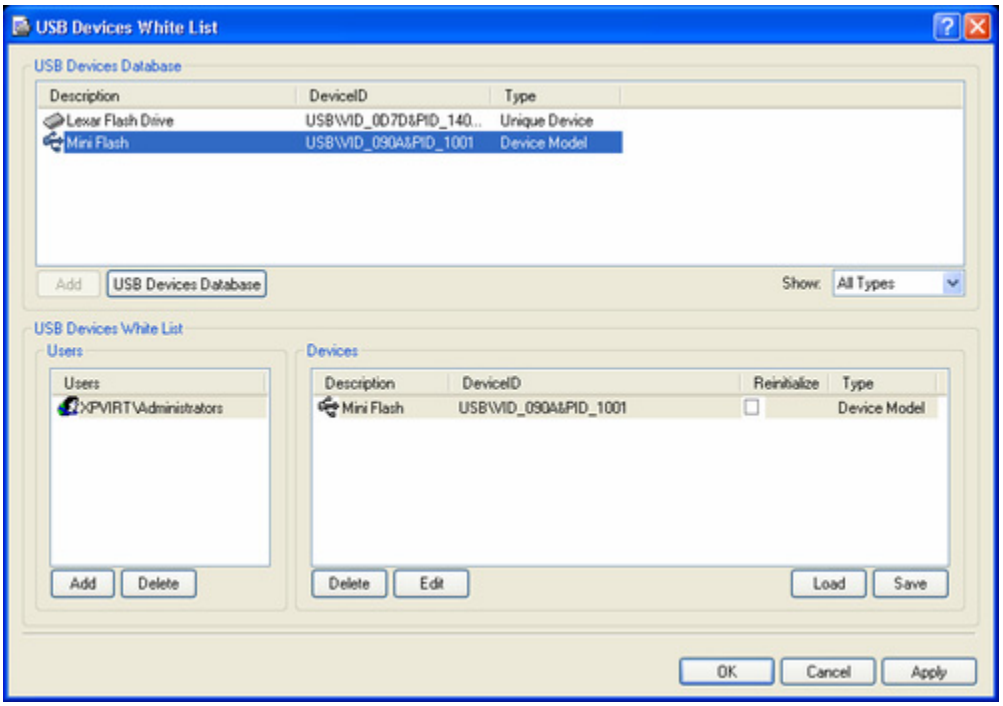
6. Fare clic sul pulsante **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**, quindi fare clic sul pulsante **Yes** per confermare la scelta.

Impedire a qualsiasi utente l'utilizzo delle periferiche USB ad eccezione della tastiera e del mouse, ma consentire ai membri del gruppo Administrators l'utilizzo di un modello di periferica di archiviazione USB autorizzata:

1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse su **USB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (per aggiungere l'utente, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e disattivare tutti i diritti nell'elenco **User's Rights**.
3. Fare clic sul pulsante **Security Settings** nella finestra di dialogo **Permissions** e quindi deselezionare la casella di controllo **Access control for USB HID (mouse, keyboard, etc.)**, come mostrato nella seguente immagine.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Fare clic sul pulsante **OK** per chiudere la finestra di dialogo **Security Settings** e quindi fare clic sul pulsante **USB White List** nella finestra di dialogo **Permissions**.



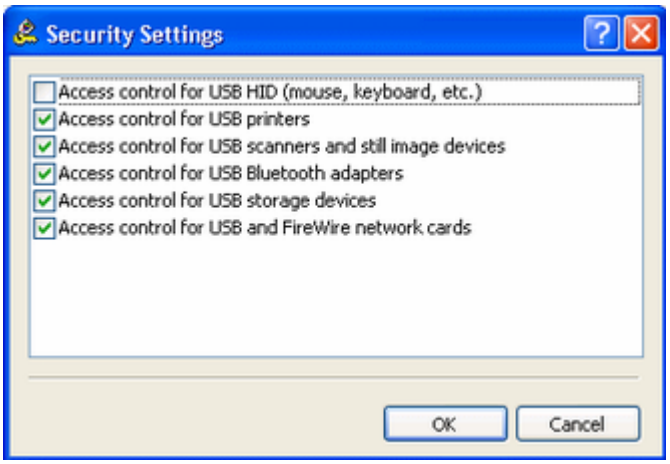
5. Fare clic sul pulsante **Add** sotto l'elenco **Users**, aggiungere il gruppo **Administrators** (per aggiungere un gruppo, digitarne il nome o selezionarlo dall'elenco degli account disponibili), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups** e quindi evidenziare la voce **Administrators**.
6. Evidenziare la voce relativa al modello della periferica nell'elenco **USB Devices Database** e quindi fare clic sul pulsante **Add** visibile sotto questo elenco.

   Se l'elenco **USB Devices Database** risulta vuoto, fare clic sul pulsante **USB Devices Database** visibile sotto l'elenco e quindi aggiungere le periferiche come descritto in Sezione USB Devices Database. Una volta aggiunte le periferiche al database, fare clic su **OK** per salvare il database e chiudere la finestra di dialogo **USB Devices Database**.

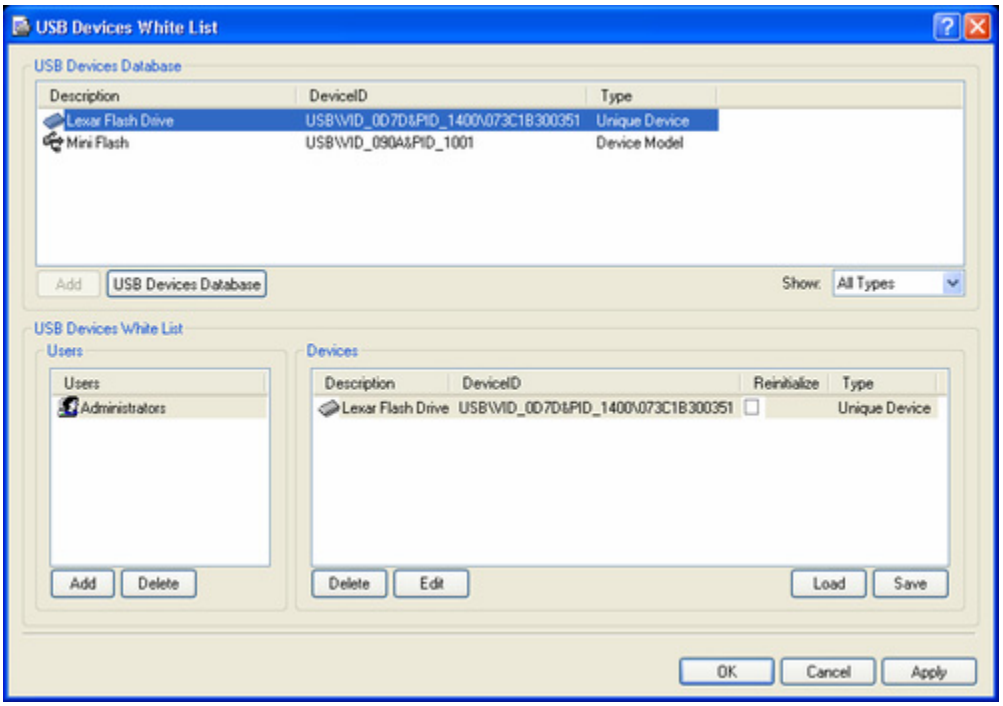
7. Fare clic sul pulsante **OK** per applicare le impostazioni alla white list e chiudere la finestra di dialogo **USB Devices White List**, scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**, quindi fare clic sul pulsante **Yes** per confermare la scelta.

Impedire a qualsiasi utente l'utilizzo delle periferiche USB ad eccezione della tastiera e del mouse, ma consentire ai membri del gruppo Administrators l'utilizzo di un modello di periferica di archiviazione USB autorizzata univoca:

1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse su **USB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (per aggiungere l'utente, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e disattivare tutti i diritti nell'elenco **User's Rights**.
3. Fare clic sul pulsante **Security Settings** nella finestra di dialogo **Permissions** e quindi deselezionare la casella di controllo **Access control for USB HID (mouse, keyboard, etc.)**, come mostrato nella seguente immagine.


Security Settings
Access control for USB HID (mouse, keyboard, etc.)
Access control for USB printers
Access control for USB scanners and still image devices
Access control for USB Bluetooth adapters
Access control for USB storage devices
Access control for USB and FireWire network cards
OK
Cancel

4. Fare clic sul pulsante **OK** per chiudere la finestra di dialogo **Security Settings** e quindi fare clic sul pulsante **USB White List** nella finestra di dialogo **Permissions**.



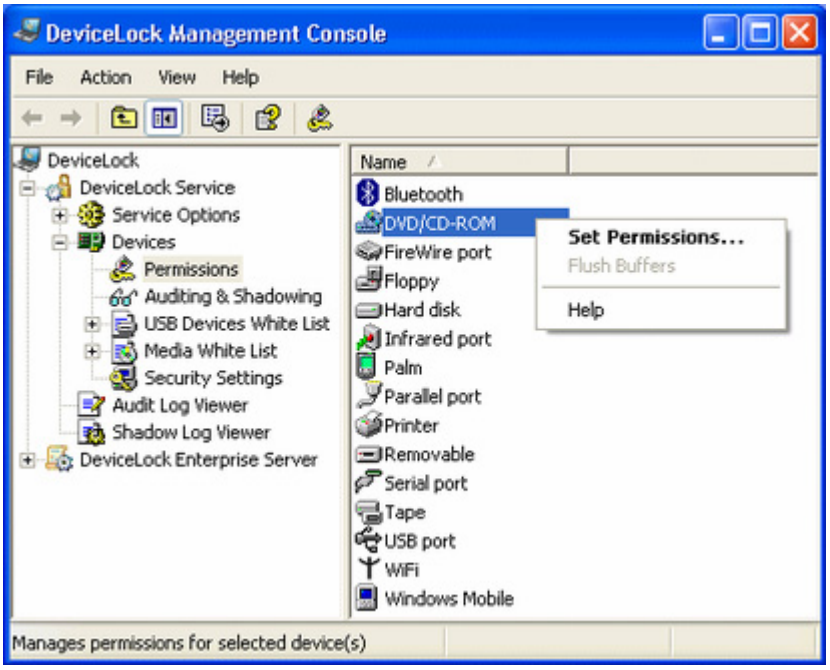
5. Fare clic sul pulsante **Add** sotto l'elenco **Users**, aggiungere il gruppo **Administrators** (per aggiungere un gruppo, digitarne il nome o selezionarlo dall'elenco degli account disponibili), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups** e quindi evidenziare la voce **Administrators**.
6. Evidenziare la voce relativa alla periferica univoca nell'elenco **USB Devices Database** e quindi fare clic sul pulsante **Add** visibile sotto questo elenco.

   Se l'elenco **USB Devices Database** risulta vuoto, fare clic sul pulsante **USB Devices Database** visibile sotto l'elenco e quindi aggiungere le periferiche come descritto in Sezione USB Devices Database. Una volta aggiunte le periferiche al database, fare clic su **OK** per salvare il database e chiudere la finestra di dialogo **USB Devices Database**.

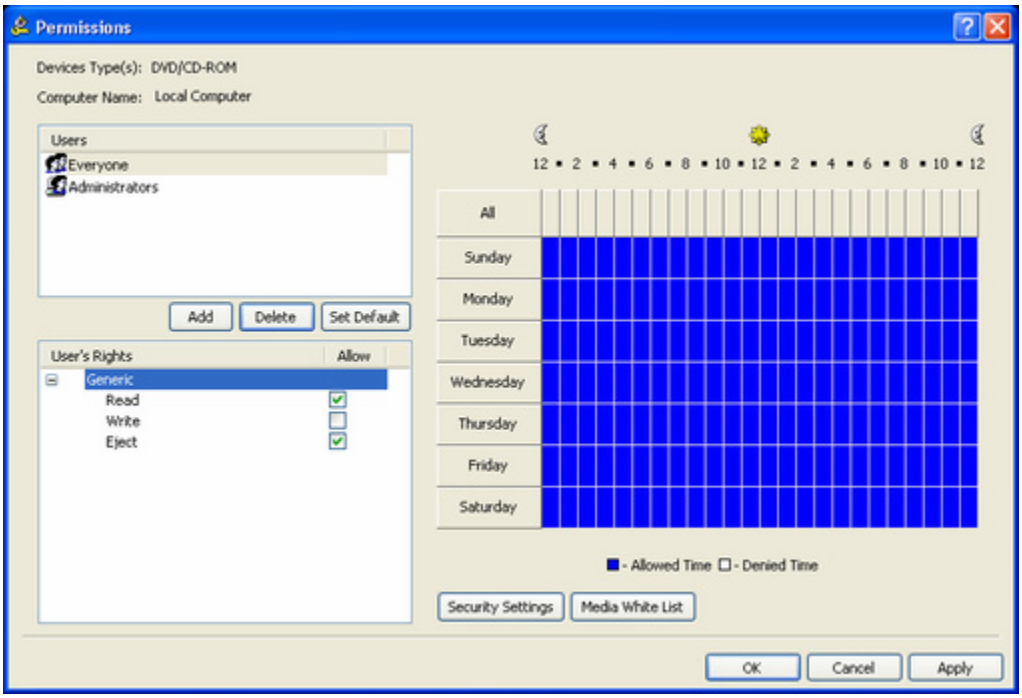
7. Fare clic sul pulsante **OK** per applicare le impostazioni alla white list e chiudere la finestra di dialogo **USB Devices White List**, scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**, quindi fare clic sul pulsante **Yes** per confermare la scelta.

Consentire a qualsiasi utente l'accesso alle unità CD e DVD in sola lettura, ma consentire ai membri del gruppo Administrators l'accesso alle unità CD e DVD in scrittura (scrittura sui dischi):

1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse sulla voce DVD/CD-ROM nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.



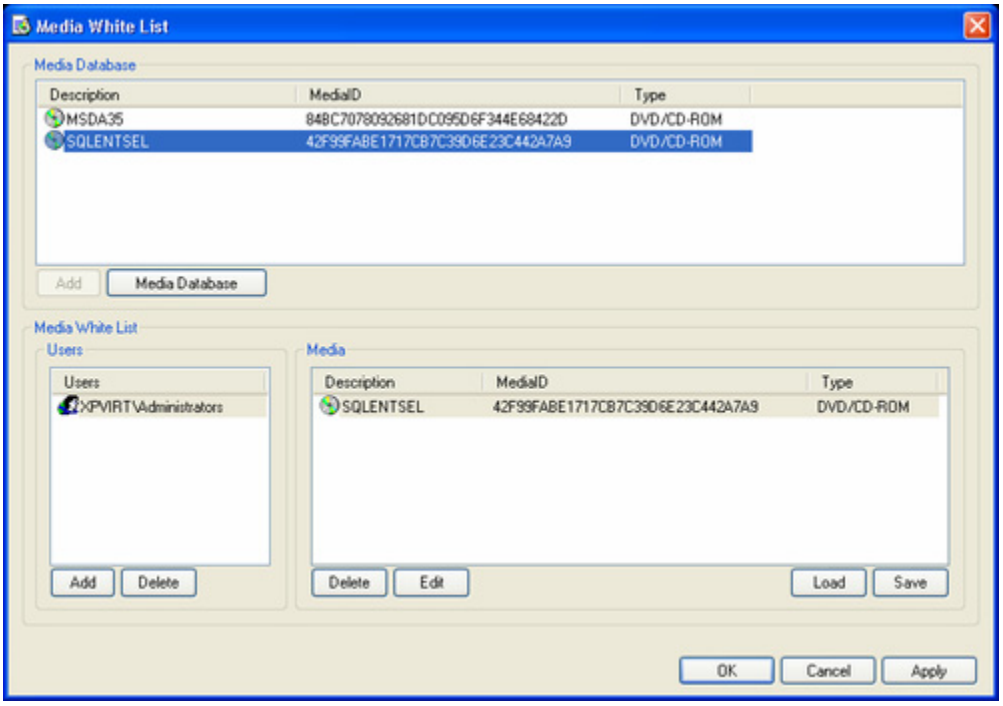
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere il gruppo **Administrators** (per aggiungere un gruppo, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Administrators** e attivare tutti i diritti nell'elenco **User's Rights**.
3. Fare clic sul pulsante Add nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (per aggiungere l'utente, digitarne il nome o selezionarlo dall'elenco degli account disponibili), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**. Selezionare la voce **Everyone** e disattivare il diritto **Write** nell'elenco **User's Rights**.



4. Fare clic su **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**.

Impedire a qualsiasi utente l'accesso alle unità CD e DVD, ma consentire ai membri del gruppo Administrators la lettura di un determinato disco:

1. Selezionare la sezione **Permissions**, fare clic con il pulsante destro del mouse sulla voce **DVD/CD-ROM** nell'elenco dei tipi di periferica e quindi scegliere **Set Permissions** dal menu sensibile al contesto.
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Permissions**, aggiungere l'utente **Everyone** (per aggiungere l'utente, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e disattivare tutti i diritti nell'elenco **User's Rights**.
3. Fare clic sul pulsante **Media White List** nella finestra di dialogo **Permissions**.



4. Fare clic sul pulsante **Add** visibile sotto l'elenco **Users**, aggiungere il gruppo **Administrators** (per aggiungere un gruppo, digitarne il nome o selezionarlo dall'elenco degli account disponibili), fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, quindi evidenziare la voce **Administrators**.
5. Evidenziare la voce relativa al disco nell'elenco **Media Database** e quindi fare clic sul pulsante **Add** visibile sotto questo elenco.

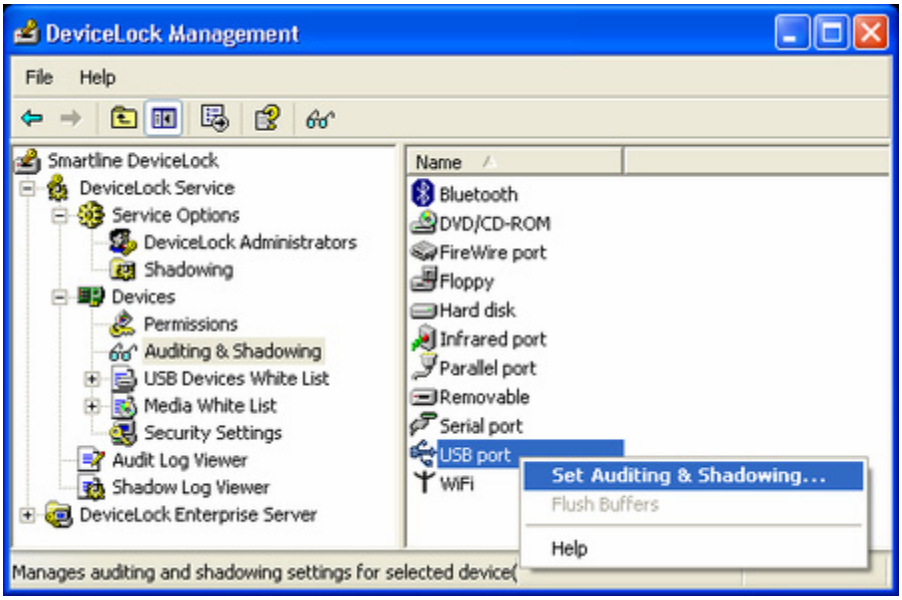
   Se l'elenco **Media Database** risulta vuoto, fare clic sul pulsante **Media Database** visibile sotto l'elenco e quindi autorizzare un supporto come descritto nella sezione Finestra di dialogo Media Database. Una volta autorizzato un disco, fare clic sul pulsante **OK** per salvare il database e chiudere la finestra di dialogo **Media Database**.

6. Fare clic sul pulsante **OK** per applicare le impostazioni alla white list e chiudere la finestra di dialogo **Media White List**, scegliere **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Permissions**, quindi fare clic sul pulsante **Yes** per confermare la scelta.

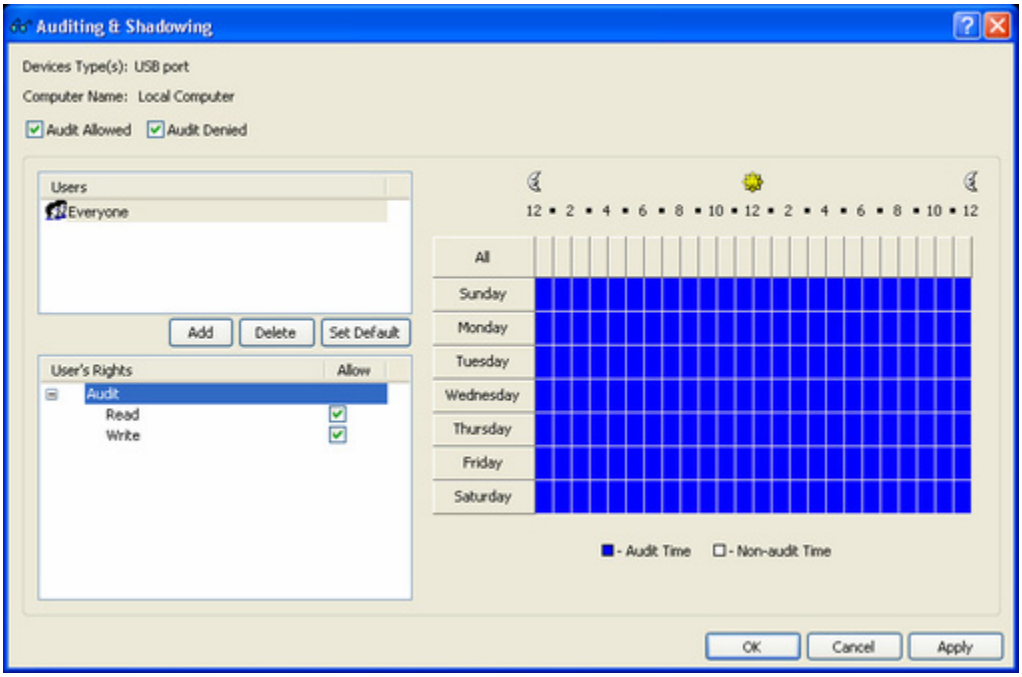
Esempi di regole di controllo e di shadowing

Memorizzare nel registro eventi le azioni di inserimento, rimozione e accesso alle periferiche USB effettuate da qualsiasi utente:

1. Selezionare la sezione **Auditing & Shadowing**, fare clic con il pulsante destro del mouse sulla voce U**SB port** nell'elenco dei tipi di periferica e quindi scegliere **Set Auditing & Shadowing** dal menu sensibile al contesto.



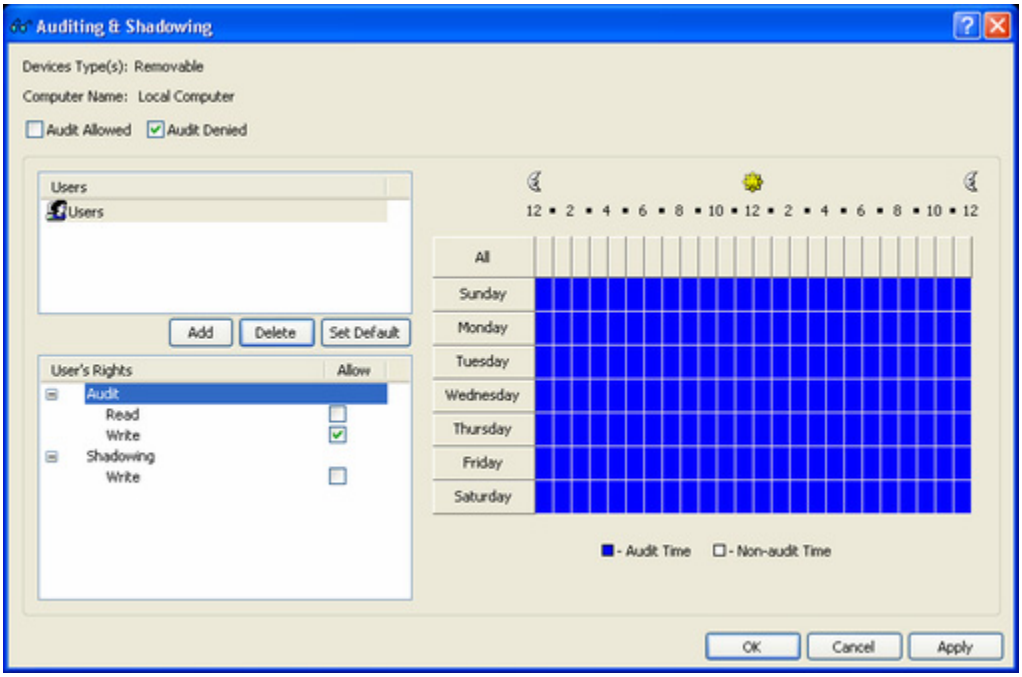
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Audit**, aggiungere l'utente **Everyone** (per aggiungere l'utente, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Everyone** e attivare i diritti di controllo **Read** e **Write** nell'elenco **User's Rights**.



3. Selezionare le caselle di controllo **Audit Allowed** e **Audit Denied** nella parte superiore della finestra di dialogo **Audit**, quindi fare clic sul pulsante **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Auditing & Shadowing**.

Memorizzare nel registro eventi solamente i nomi di file e cartelle relativi alle azioni di scrittura negate sulle periferiche di archiviazione rimovibili effettuate dal gruppo Users:

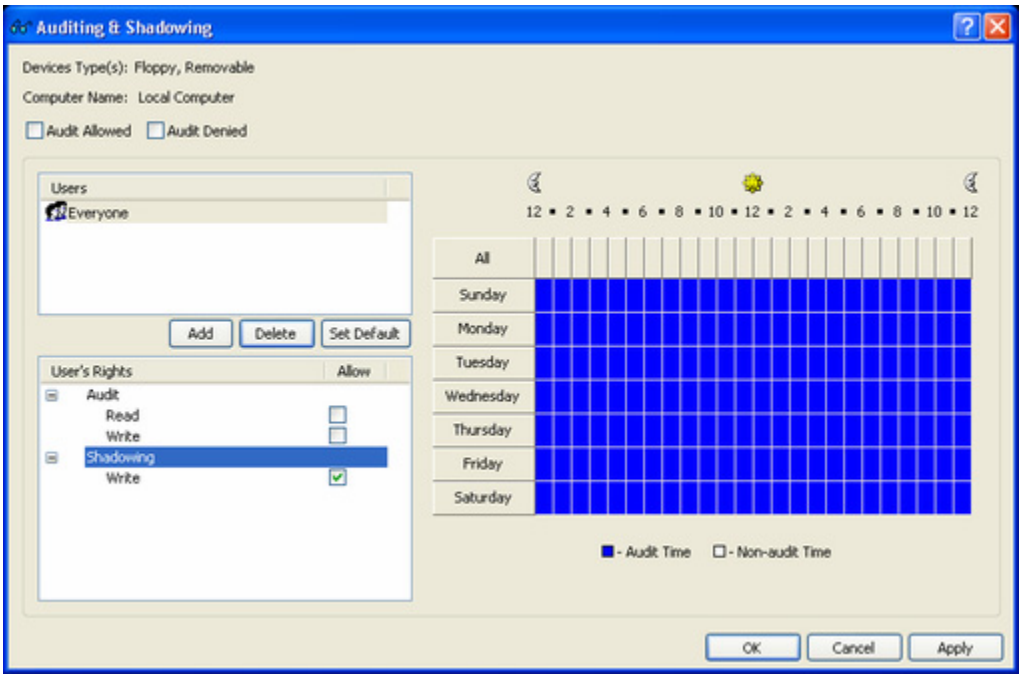
1. Selezionare la sezione **Auditing & Shadowing**, fare clic con il pulsante destro del mouse sulla voce **Removable** nell'elenco dei tipi di periferica e quindi scegliere **Set Auditing & Shadowing** dal menu sensibile al contesto.
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Audit**, aggiungere il gruppo **Users** (per aggiungere un gruppo, digitarne il nome o selezionarlo dall'elenco degli account disponibili). Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups**, selezionare la voce **Users** e attivare solo il diritto di controllo **Write** nell'elenco **User's Rights**.



3. Selezionare solamente la casella di controllo **Audit Denied** nella parte superiore della finestra di dialogo **Audit**, quindi fare clic sul pulsante **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Auditing & Shadowing**.

Creare le copie di shadow dei dati scritti da qualsiasi utente sulle periferiche di archiviazione rimovibili e sulle unità floppy:

1. Selezionare le voci **Floppy** e **Removable** dall'elenco dei tipi di periferica in **Auditing & Shadowing**, quindi selezionare **Set Auditing & Shadowing** dal menu contestuale disponibile facendo clic con il pulsante destro del mouse.
2. Fare clic sul pulsante **Add** nella finestra di dialogo **Audit** e aggiungere l'utente **Everyone**. Fare clic su **OK** per chiudere la finestra di dialogo **Select Users or Groups** e selezionare la voce **Everyone**. Disattivare tutti i diritti di controllo e attivare solo il diritto di shadowing **Write** nell'elenco **User's Rights**.

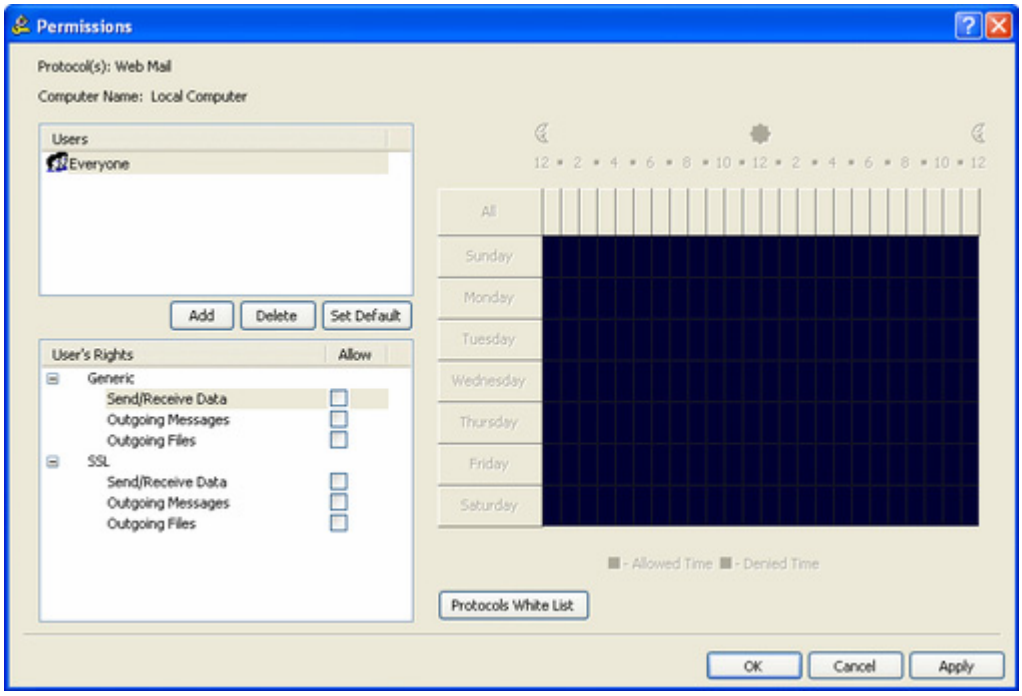


3. Fare clic su **OK** per applicare le modifiche apportate e chiudere la finestra di dialogo **Auditing & Shadowing**.

Esempi di autorizzazioni per i protocolli

I servizi di Webmail vengono negati a tutti gli utenti, mentre i membri del gruppo Administrators possono accedere a Gmail:

1. Nella struttura della console, espandere **DeviceLock Service**, quindi **Protocols**.
2. Sotto **Protocols**, selezionare **Permissions**.
3. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su **Web Mail**, quindi selezionare **Set Permissions**.
4. Nella finestra di dialogo **Permissions**, attenersi alle seguenti istruzioni:
    a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Everyone**, quindi fare clic su **OK**.
    b) Sotto **Users**, selezionare **Everyone**.
    c) Sotto **User's Rights**, deselezionare tutte le caselle di controllo per disattivare tutti i diritti.

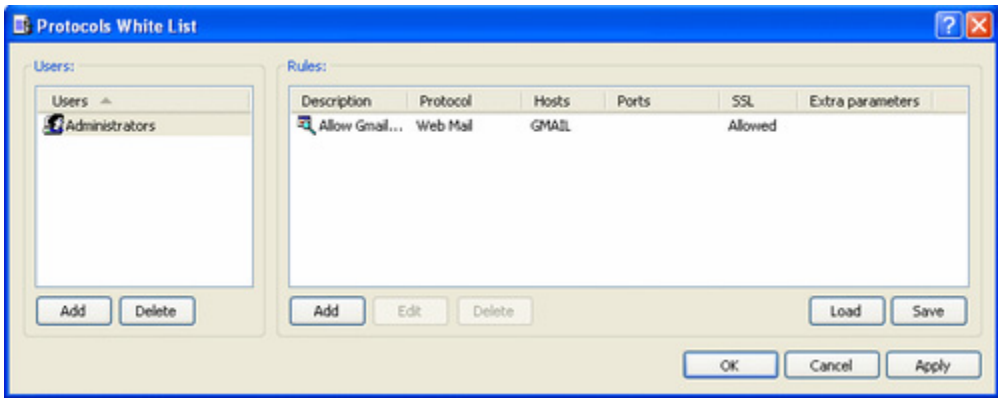


d) Fare clic su **Protocols White List**.

5. Nella finestra di dialogo **Protocols White List**, attenersi alle seguenti istruzioni:

   a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Administrators**, quindi fare clic su **OK**.

   b) Sotto **Users**, selezionare **Administrators**; in seguito, sotto **Rules**, fare clic su **Add**. Nella finestra di dialogo **Add Rule**, nella casella **Description**, specificare il nome della regola. In seguito, sotto **Web Mail services**, selezionare la casella di controllo **Gmail** e fare clic su **OK**.

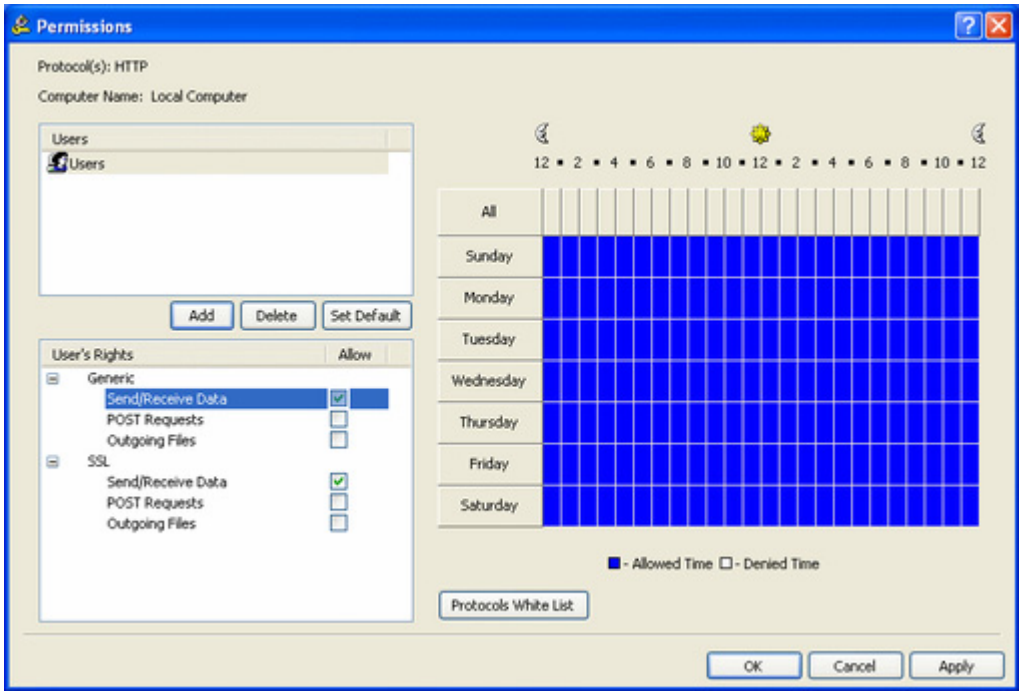


   c) Fare clic su **OK** o su **Apply** per applicare le impostazioni della lista bianca e chiudere la finestra di dialogo **Protocols White List**.

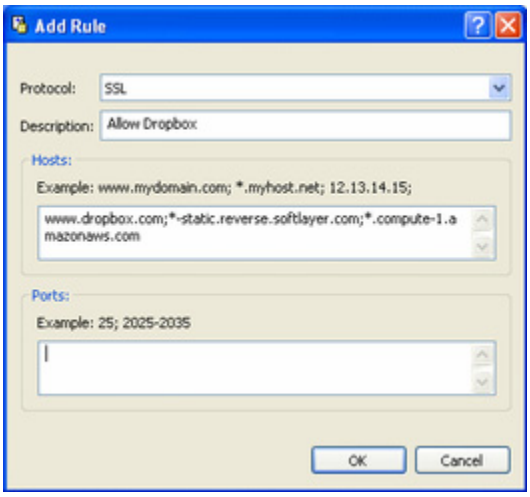
6. Nella finestra di dialogo **Permissions**, fare clic su **OK** o su **Apply**.

I membri del gruppo Users sono autorizzati a utilizzare Dropbox:

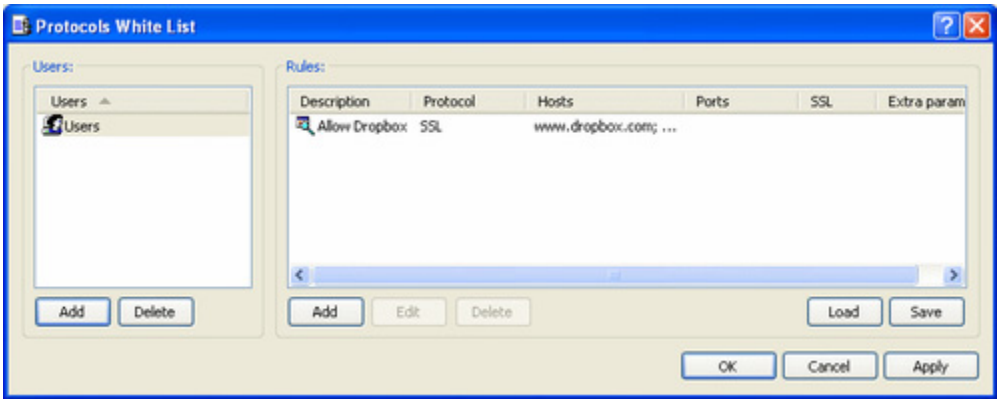
1. Nella struttura della console, espandere **DeviceLock Service**, quindi **Protocols**.
2. Sotto **Protocols**, selezionare **Permissions**.
3. Nel riquadro dei dettagli, fare clic con il pulsante destro del mouse su **HTTP**, quindi selezionare **Set Permissions**.
4. Nella finestra di dialogo **Permissions**, attenersi alle seguenti istruzioni:
   a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Users**, quindi fare clic su **OK**.
   b) Sotto **Users**, selezionare **Users**.
   c) Sotto **User's Rights**, selezionare le caselle di controllo poste accanto ai seguenti diritti: **Generic: Send/Receive Data** e **SSL: Send/Receive Data**.



   d) Fare clic su **Protocols White List**.
5. Nella finestra di dialogo **Protocols White List**, attenersi alle seguenti istruzioni:
   a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Users**, quindi fare clic su **OK**.
   b) Sotto **Users**, selezionare **Users**; in seguito, sotto **Rules**, fare clic su **Add**.
6. Nella finestra di dialogo **Add Rule**, attenersi alle seguenti istruzioni:
   a) Nell'elenco **Protocol:**, fare clic su **SSL**.
   b) Nella casella **Description**, specificare il nome della regola.
   c) Nella casella **Hosts:**, digitare i nomi dei DNS dei server di Dropbox separati da una virgola o da un punto e virgola: **www.dropbox.com; *-static.reverse.softlayer.com; *.compute-1.amazonaws.com**.



d) Fare clic su **OK**.



7. Fare clic su **OK** o su **Apply** per applicare le impostazioni della lista bianca e chiudere la finestra di dialogo **Protocols White List**.
8. Nella finestra di dialogo **Permissions**, fare clic su **OK** o su **Apply**.

Nota: il controllo dell'accesso, la verifica, la copia shadow e il filtraggio del contenuto verranno disattivati per tutti i trasferimenti di file con Dropbox.

Esempi di regole basate sul contenuto (Content-Aware Rules)

Nessun utente è autorizzato a copiare sulle periferiche (Floppy, Removable) e a trasmettere sulla rete (su HTTP, FTP, SMTP e Web Mail) i seguenti contenuti: file contenenti più di 1 numero di carta di credito, documenti e archivi protetti da password, file contenenti più di 1 numero di Social Security e immagini contenenti grandi quantità di testo.

1. Nella struttura della console, espandere **DeviceLock Service**, espandere **Devices**, fare clic con il pulsante destro del mouse su **Content-Aware Rules** e selezionare **Manage**.

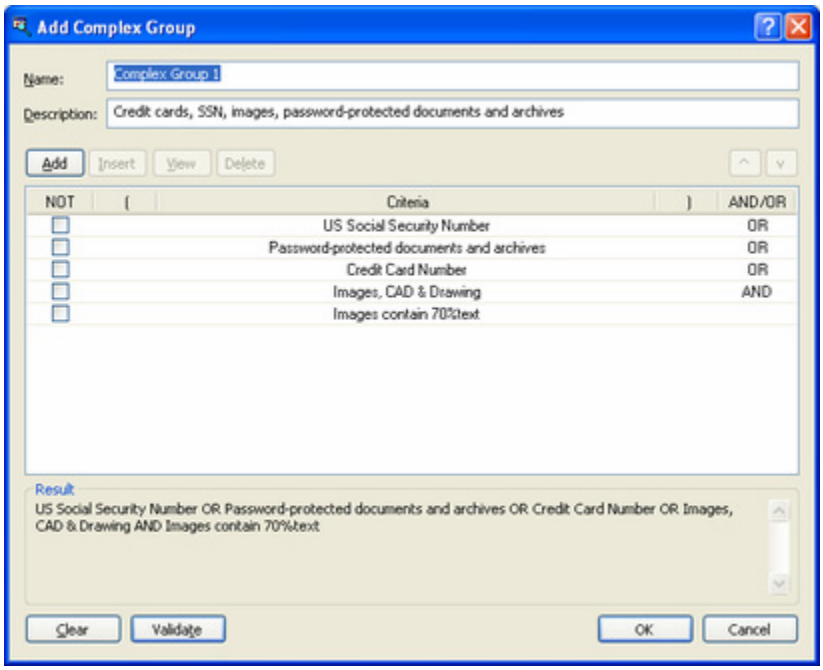
2. Nella finestra di dialogo **Content-Aware Rules for Devices**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Document Properties**.
3. Nella finestra di dialogo **Add Document Properties Group**, attenersi alle seguenti istruzioni:
    a) Nella finestra **Name**, specificare il nome del gruppo, ad esempio **Password-protected documents and archives**.
    b) Selezionare la casella di controllo **Password protected**.
    c) Fare clic su **OK**.

    Il gruppo di contenuto appena creato viene aggiunto all'elenco esistente dei gruppi di contenuto, sotto Content Database, nella finestra di dialogo Content-Aware Rules for Devices. Questo gruppo verrà utilizzato per controllare l'accesso ai documenti e agli archivi protetti da password.

4. Nella finestra di dialogo **Content-Aware Rules for Devices**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Document Properties**.
5. Nella finestra di dialogo **Add Document Properties Group**, attenersi alle seguenti istruzioni:
    a) Nella finestra **Name**, specificare il nome del gruppo, ad esempio **Images contain 70%text**.
    b) Selezionare la casella di controllo **Contains text** e specificare **70 %**.
    c) Fare clic su **OK**.

    Il gruppo di contenuto appena creato viene aggiunto all'elenco esistente dei gruppi di contenuto, sotto Content Database, nella finestra di dialogo Content-Aware Rules for Devices. Questo gruppo verrà utilizzato per controllare l'accesso alle immagini contenenti grandi quantità di testo.

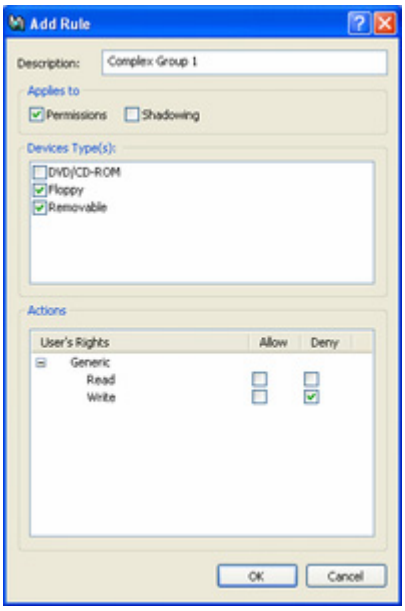
6. Nella finestra di dialogo **Content-Aware Rules for Devices**, sotto **Content Database**, fare clic sulla freccia di selezione accanto ad **Add Group** e selezionare **Complex**.
7. Nella finestra di dialogo **Add Complex Group**, attenersi alle seguenti istruzioni:
    a) Nella finestra **Name**, specificare il nome del gruppo, ad esempio **Complex Group 1**.
    b) Fare clic su **Add**. Nella finestra di dialogo **Content Groups**, selezionare i seguenti gruppi: **Credit Card Number**, **Images, CAD & Drawing**, **Images contain 70%text**, **Password-protected documents and archives** e **US Social Security Number**.
    È possibile selezionare questi gruppi simultaneamente tenendo premuto il tasto CTRL mentre si fa clic sui gruppi.
    c) Comporre la seguente espressione logica: **US Social Security Number OR Password-protected documents and archives OR Credit Card Number OR Images, CAD & Drawing AND Images contain 70%text**.



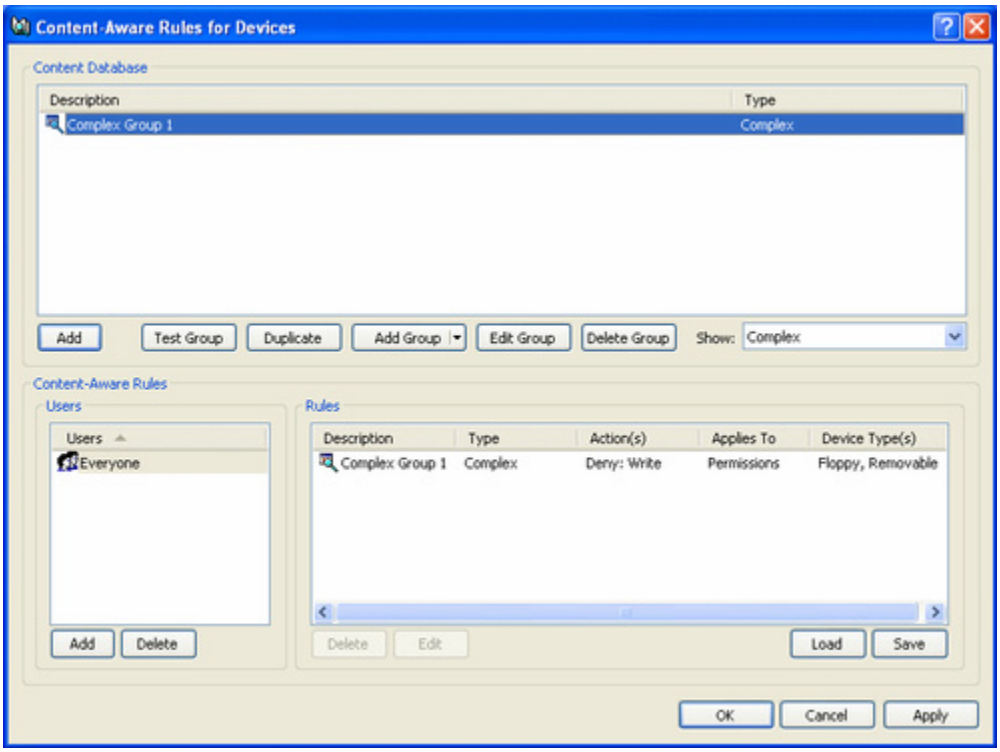
d) Fare clic su **OK**.

Il gruppo di contenuto appena creato viene aggiunto all'elenco esistente dei gruppi di contenuto, sotto Content Database, nella finestra di dialogo Content-Aware Rules for Devices. Questo gruppo verrà utilizzato per controllare l'accesso ai file contenenti più di 1 numero di carta di credito, ai documenti e agli archivi protetti da password, ai file contenenti più di 1 numero di Social Security e alle immagini contenenti grandi quantità di testo.

8. Nella finestra di dialogo **Content-Aware Rules for Devices**, attenersi alle seguenti istruzioni:
   a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Everyone**, quindi fare clic su **OK**.
   b) Sotto **Users**, selezionare **Everyone**. Sotto **Content Database**, selezionare il gruppo di contenuto **Complex Group 1** e fare clic su **Add**.
9. Nella finestra di dialogo **Add Rule**, attenersi alle seguenti istruzioni:
   a) Sotto **Applies to**, selezionare la casella di controllo **Permissions**.
   b) Sotto **Device Type(s)**, selezionare le caselle di controllo **Floppy** e **Removable**.
   c) Sotto **Action(s)**, selezionare la casella di controllo **Deny** posta accanto a **Write**.



d) Fare clic su **OK**.

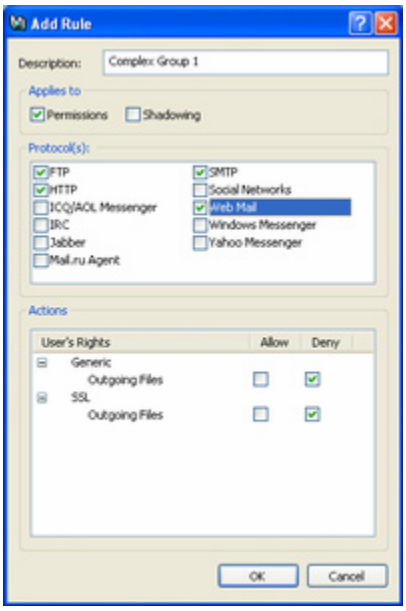


10. Nella finestra di dialogo **Content-Aware Rules for Devices**, fare clic su **OK** o su **Apply** per applicare la regola.
11. Nella struttura della console, espandere **Protocols**, fare clic con il pulsante destro del mouse su **Content-Aware Rules** e selezionare **Manage**.
12. Nella finestra di dialogo **Content-Aware Rules for Protocols**, attenersi alle seguenti istruzioni:

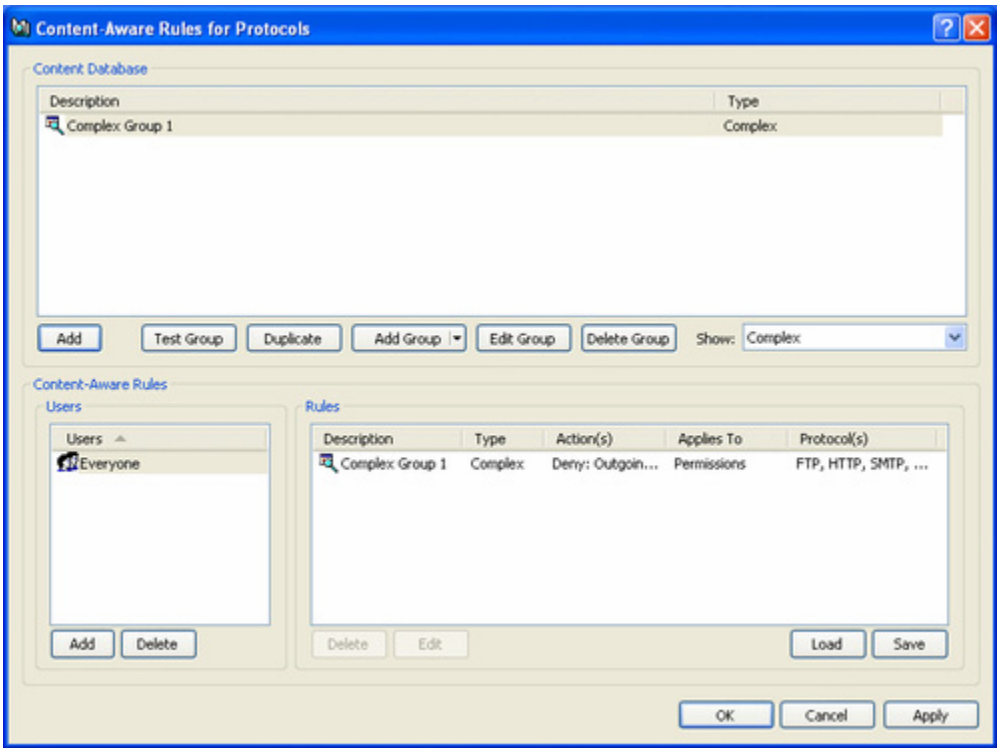
a) Sotto **Users**, fare clic su **Add**. Nella finestra di dialogo **Select Users or Groups**, nella casella **Enter the object names to select**, digitare **Everyone**, quindi fare clic su **OK**.
b) Sotto **Users**, selezionare **Everyone**. Sotto **Content Database**, selezionare il gruppo di contenuto **Complex Group 1** e fare clic su **Add**.

13. Nella finestra di dialogo **Add Rule**, attenersi alle seguenti istruzioni:

a) Sotto **Applies to**, selezionare la casella di controllo **Permissions**.
b) Sotto **Protocol(s)**, selezionare le caselle di controllo **FTP**, **HTTP**, **SMTP** e **Web Mail**.
c) Sotto **Action(s)**, selezionare la casella di controllo **Deny** posta accanto a **Generic: Outgoing Files** e **SSL: Outgoing Files**.



d) Fare clic su **OK**.



14. Nella finestra di dialogo **Content-Aware Rules for Protocols**, fare clic su **OK** o su **Apply** per applicare la regola.